安裝指南

Novell®
Sentinel 6.1 Rapid Deployment

SP2

2011 年 4 月

www.novell.com

N®

法律聲明

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

*線上文件：*若要存取本產品及其他 Novell 產品的最新線上文件，請參閱 Novell 文件網頁 (http://www.novell.com/documentation)。

Novell 商標

協力廠商資料

目錄

關於本指南

本指南旨在簡單介紹 Novell Sentinel 6.1 Rapid Deployment Service Pack 2，並說明其安裝程序。

使用對象

本文件適用於 「資訊安全專業人員」。

意見反應

我們希望得到您對本手冊以及本產品隨附之其他文件的意見和建議。請使用線上文件每頁下方的使用備註功能，並在其中輸入您的意見。

其他文件

Sentinel 技術文件分為數冊。它們是：

- *Novell Sentinel Rapid Deployment 安裝指南* (http://www.novell.com/documentation/sentinel61rd/s61rd_install/data/index.html)
- *Novell Sentinel Rapid Deployment 使用者指南* (http://www.novell.com/documentation/sentinel61rd/s61rd_user/data/bookinfo.html)
- *Novell Sentinel Rapid Deployment 參考指南* (http://www.novell.com/documentation/sentinel61rd/s61rd_reference/data/bookinfo.html)
- *Novell Sentinel 安裝指南* (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/)
- *Novell Sentinel User Guide (Novell Sentinel 使用者指南)* (http://www.novell.com/documentation/sentinel61/s61_user/?page=/documentation/sentinel61/s61_user/data/)
- *Novell Sentinel 參考指南* (http://www.novell.com/documentation/sentinel61/s61_reference/?page=/documentation/sentinel61/s61_reference/data/)
- *Sentinel SDK* (http://www.novell.com/developer/develop_to_sentinel.html)

  Sentinel SDK 網站提供開發收集器 (專屬或 JavaScript) 以及 JavaScript 關連動作的詳細資料。

連絡 Novell

- *Novell 網站* (http://www.novell.com)
- *Novell 技術支援 (NTS)* (http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup)
- *Novell 自助支援* (http://support.novell.com/support_options.html?sourceidint=suplnav_supportprog)
- *修補程式下載網站* (http://download.novell.com/index.jsp)
- *Novell 24x7 支援* (http://www.novell.com/company/contact.html)
- *Sentinel TIDS* (http://support.novell.com/products/sentinel)
- Sentinel 社群支援論壇 (http://forums.novell.com/novell-product-support-forums/sentinel/)
- Sentinel 外掛程式網站 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html)
- 通知電子郵件清單：透過 Sentinel 外掛程式網站註冊

產品綜覽 1

Sentinel 6.1 Rapid Deployment 是 Novell Sentinel 的精簡版，它採用開放原始碼的 PostgreSQL、activeMQ 與 JasperReports 元件。

以下各節可協助您瞭解 Sentinel 6.1 Rapid Deployment 系統的主要元件。本 《*Sentinel Rapid Deployment 安裝指南*》提供了安裝和組態程序的詳細資訊。《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) (http://www.novell.com/documentation/sentinel61rd/s61rd_user/?page=/documentation/sentinel61rd/s61rd_user/data/bookinfo.html) 內含更詳細的架構、操作和管理程序。

1.1 Sentinel 6.1 Rapid Deployment 綜覽

Sentinel 是一套安全性資訊與事件管理解決方案，可接收來自企業內許多來源的資訊，將其標準化並排定優先順序之後，再供您用於制訂與威脅、風險和規則相關的決策。

Sentinel 可自動化記錄收集、分析和報告程序，以確保 IT 控制能有效支援威脅偵測與稽核要求。Sentinel 以自動化的連續方式，監控安全性與法規遵循事件及 IT 控制，取代了勞力密集的手動程序。

Sentinel 還會從組織的網路基礎架構以及協力廠商系統、設備與應用程式，收集和關連安全性與非安全性資訊。Sentinel 以圖形化介面來呈現所收集的資料，辨識安全性或法規遵循問題，並追蹤矯正活動，將容易出錯的程序簡化，建立嚴密安全的管理程式。

自動的事件回應管理可讓您將追蹤、提報和回應事件與違反規則的程序作成記錄並形式化，提供與問題報修系統的雙向整合。Sentinel 可讓您即時回應，以有效率的方式解決事件。

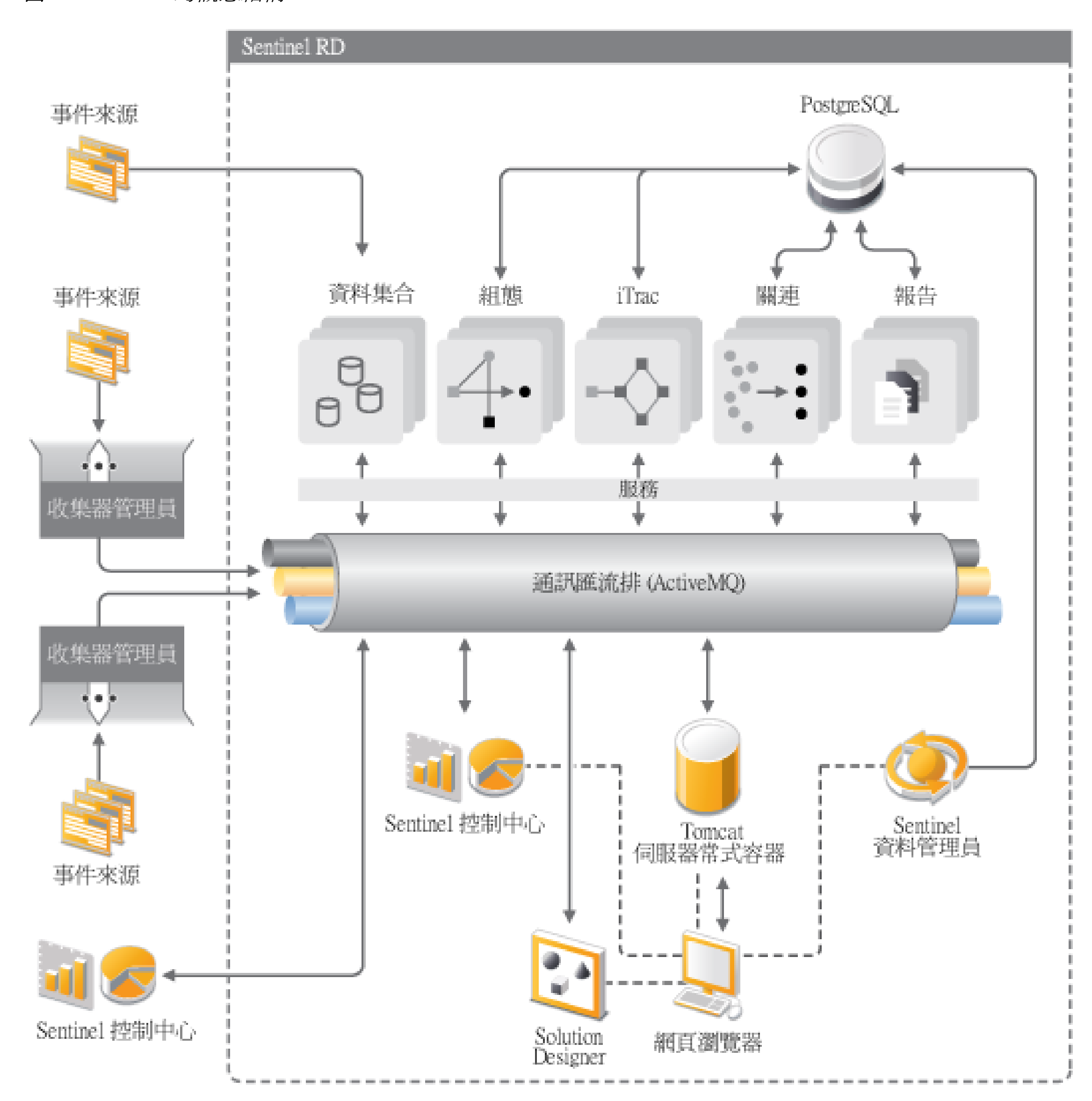
「解決方案套件」可輕輕鬆鬆配送 Sentinel 關連規則、動態清單、映射、報告與 iTRAC 工作流程，並將其輸入控制項。這些控制項可以根據特定的法規要求 (例如 《支付卡產業之資料安全標準》) 加以設計，或是針對特定資料來源 (例如針對資料庫的使用者驗證事件) 建立相關性。

憑藉 Sentinel Rapid Deployment，您便可：

- 在所有系統和網路之間進行整合性的自動化即時安全性管理和法規遵循監控作業。
- 擁有得以推動 IT 規則與行動的企業規則架構。
- 針對全企業的安全性、系統與存取事件，自動進行記錄與報告。
- 進行內建的事件管理和補救作業。
- 展示並監控內部規則及政府法規 (例如 「沙賓法案」、HIPAA、GLBA 及 FISMA) 的遵循狀況。實作這些控制項所需的內容透過解決方案套件加以配送和實作。

以下是 Sentinel Rapid Deployment 之概念架構的圖例，其中顯示了執行安全性與法規遵循管理的相關元件。

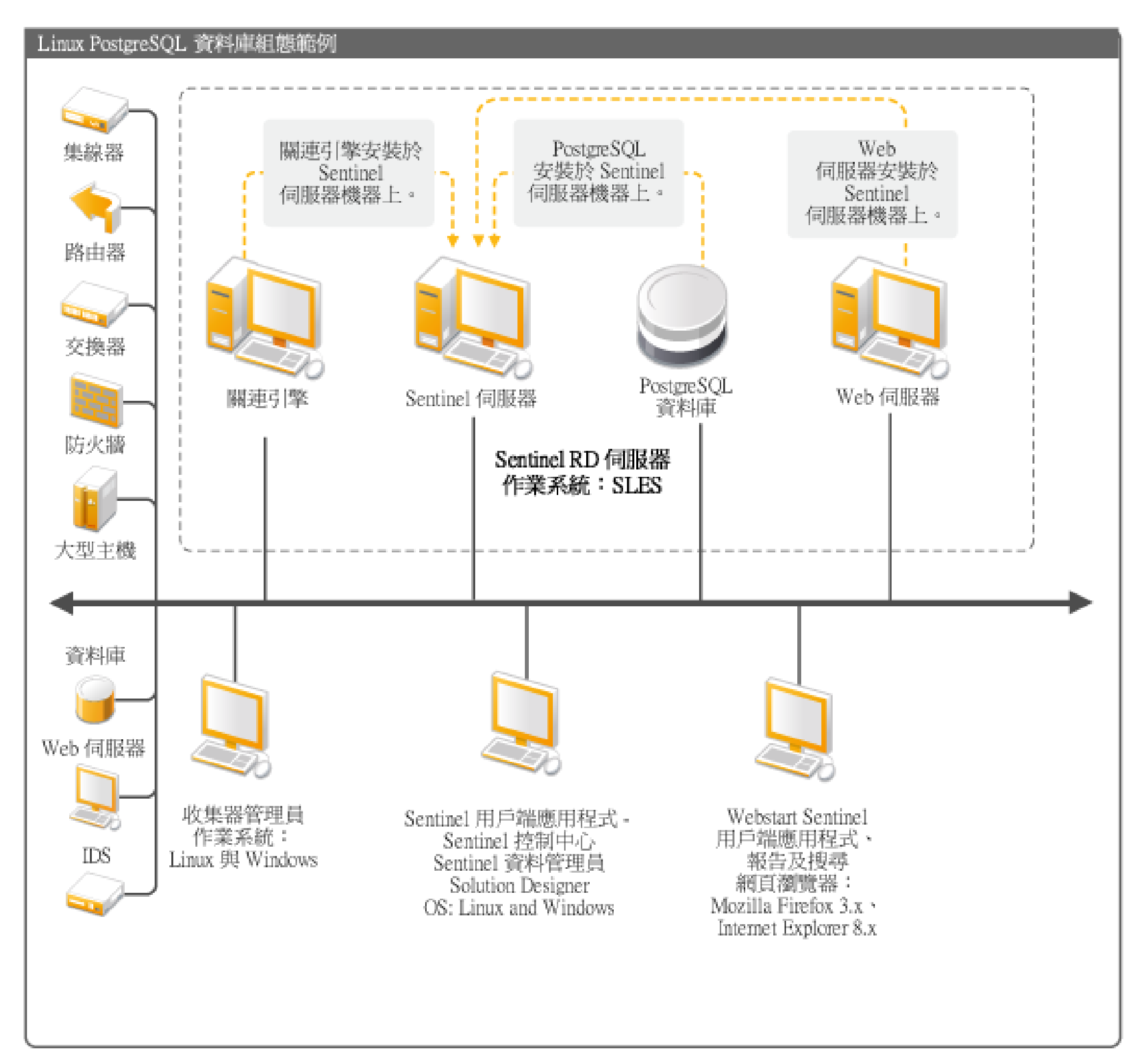
圖 1-1　Sentinel 的概念結構



1.2 Sentinel 6.1 Rapid Deployment 組態

下圖說明了 Sentinel 6.1 Rapid Deployment 的組態設定。

圖 1-2 Sentinel 6.1 Rapid Deployment 組態



1.3 Sentinel Rapid Deployment 使用者介面

Sentinel 包含下列容易使用的使用者介面：

- Sentinel 6.1 Rapid Deployment Web 介面
- Sentinel 控制中心
- Sentinel 資料管理員
- Sentinel Solution Designer
- Sentinel Plug-In SDK

1.3.1 Sentinel 6.1 Rapid Deployment Web 介面

您可以使用 Novell Sentinel 6.1 Rapid Deployment Web 介面來管理報告，以及啟動 Sentinel 控制中心 (SCC)、Sentinel 資料管理員及 Solution Designer。您也可以從 Sentinel 6.1 Rapid Deployment Web 介面的 「*應用程式*」頁面下載 「收集器管理員」安裝程式與用戶端安裝程式。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Managing Sentinel Rapid Deployment Through the Web Interface」(透過 Web 介面管理 Sentinel Rapid Deployment)。

1.3.2 Sentinel 控制中心

SCC 提供了整合式的安全性管理儀表板，可讓分析師快速地辨識新的趨勢或攻擊，且能操作並與即時圖形資訊互動，還能對事件做出反應。

您能以用戶端應用程式方式啟動 SCC 或使用 Java Webstart 來啟動 SCC。

SCC 的主要功能包括：

- **Active Views**：提供即時分析和視覺化
- **分析**： 執行和儲存離線查詢
- **事件**：提供事件的建立和管理
- **關連性**：提供關連規則定義和管理
- **iTRAC**：提供記錄、執行及追蹤事件解析程序的程序管理
- **報告**：提供歷程報告和計量
- **事件來源管理**：提供收集器部署和監控
- **解決方案管理員**：安裝、實作和測試解決方案套件內容

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Sentinel Control Center」(Sentinel 控制中心)。

1.3.3 Sentinel 資料管理員

Sentinel 資料管理員可讓您管理 Sentinel 資料庫。您可以在 Sentinel 資料管理員中執行以下操作：

- 監控資料庫空間使用率。
- 檢視與管理資料庫分割區。
- 管理資料庫歸檔。
- 將歸檔的資料輸入回資料庫。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Sentinel Data Manager」(Sentinel 資料管理員)。

1.3.4 Sentinel Solution Designer

Sentinel Solution Designer 可用來建立與修改解決方案套件，也就是套裝的 Sentinel 內容集 (例如關連規則、動作、iTRAC 工作流程及報告)。

Sentinel 內容是 Sentinel 系統的延伸功能。此內容包含 Sentinel 動作、Integrator 和 Sentinel 外掛程式 (例如，收集器、連接器及可能包含多種其他類型之外掛程式的解決方案套件)。這些模組化元件用於與協力廠商系統整合，安裝基於控制的完整安全解決方案，以及對偵測到的事件進行自動矯正。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Solution Packs」(解決方案套件)。

1.3.5 Sentinel Plug-In SDK

Sentinel 外掛程式 SDK 包含 Novell Engineering 開發的程式庫與程式碼，以及可用來自行開發專案的範本與範例程式碼。如需詳細資訊，請參閱 Sentinel SDK (http://www.novell.com/developer/develop_to_sentinel.html)。

1.4 Sentinel 伺服器元件

Sentinel 由下列元件組成：

1.4.1 資料存取服務

Sentinel 資料存取服務是用來與 Sentinel 資料庫通訊的主要元件。資料存取伺服器搭配其他伺服器元件，可將自收集器管理員所接收的事件儲存至資料庫中、過濾資料、處理主動檢視顯示、執行資料庫查詢並處理結果，以及處理權限管理任務，例如使用者驗證與授權。如需詳細資訊，請參閱 《*Sentinel Rapid Deployment Reference Guide*》 (Sentinel Rapid Deployment 參考指南) 中的 「Data Access Service」(資料存取服務)。

1.4.2 訊息匯流排

Sentinel 6.1 Rapid Deployment 使用開放原始碼的訊息仲介，稱為 Apache Active MQ。訊息匯流排可以在短時間內於 Sentinel 元件之間移動數以千計的訊息封包。Apache Active MQ 架構是以 Java Message Oriented Middleware (JMOM) 為基礎，JMOM 支援用戶端與伺服器應用程式之間的非同步呼叫。當目的程式忙碌或未連接時，訊息佇列可提供暫時儲存空間。如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Communication Server」(通訊伺服器)。

1.4.3 Sentinel 資料庫

Sentinel 產品是以儲存安全性事件和所有 Sentinel 中繼資料的終端資料庫為基礎而建立的。Sentinel 6.1 Rapid Deployment 支援 PostgreSQL。事件會連同資產、漏洞資料、識別資訊、事件與工作流程狀態及其他類型的資料，以標準化格式一起儲存。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的「Sentinel Data Manager」(Sentinel 資料管理員)。

1.4.4 Sentinel 收集者管理員

Sentinel 收集器管理員可管理資料收集、監控系統狀態訊息，並視需要執行事件過濾。收集器管理員的主要功能包括轉換事件、經由分類來為事件新增業務相關性、對事件執行全域過濾、路由事件並傳送狀態訊息至 Sentinel 伺服器。「Sentinel 收集器管理員」會直接連接到訊息匯流排。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Collector Manager」(收集器管理員)。

1.4.5 Correlation Engine (關聯性引擎)

關連引擎會自動分析收到的事件資料流來尋找有嫌疑的模式，藉此提升安全性事件管理方面的情報完整度。您可使用關聯性來定義規則以識別嚴重威脅和複雜的攻擊模式，以便您按優先順序來處理事件並進行有效的事件管理和回應作業。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Correlation Tab」(關連索引標籤)。

1.4.6 iTRAC

Sentinel 提供 iTRAC 工作流程管理系統，以定義與自動化事件回應的程序。在 Sentinel 中利用關聯性規則或透過手動方式所識別的事件，都可以與 iTRAC 工作流程建立關聯。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「iTRAC Workflows」(iTRAC 工作流程)。

1.4.7 Sentinel Advisor 與入侵偵測

「Sentinel Advisor」為選擇性的資料訂閱服務，其中包括已知攻擊、弱點，以及矯正的資訊。本資料結合您環境的已知弱點與即時入侵偵測或預防資訊，提供主動入侵偵測，並且可以在易受威脅系統遭受攻擊時立即行動。

安裝 Sentinel 6.1 Rapid Deployment 時預設會安裝一個 Advisor 資料快照。您需要 Advisor 授權才能訂閱持續發佈的 Advisor 資料更新。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Advisor Usage and Maintenance」(Advisor 的使用與維護)。

1.4.8 網路伺服器

Sentinel Rapid Deployment 使用 Apache Tomcat 做為其 Web 伺服器，藉此確保連往 Sentinel Rapid Deployment Web 介面的連線安全無虞。

1.5 Sentinel 外掛程式

Sentinel 支援各種可擴充與增強系統功能的外掛程式。系統中會預安裝其中的一些外掛程式。其他外掛程式 (及更新) 可從 Sentinel 6.1 外掛程式網站 (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 下載。

某些外掛程式 (例如 Remedy Integrator、IBM Mainframe Connector 與 Connector for SAP XAL) 要求您必須有額外授權才能下載。

1.5.1 收集器

將關聯性和分析後的事件傳送至資料庫之前，Sentinel 會將分類法、入侵偵測和企業相關性用於資料流中，以收集來自來源裝置的資料並提供更豐富的事件資料流。更豐富的事件資料流表示該資料與所需的企業環境有關連，以便識別並矯正內外部威脅與規則違規情形。

Sentinel 收集器可剖析下列各種設備及其他的資料：

◆ 入侵偵測系統 (主機)	◆ 防毒偵測系統
◆ 入侵偵測系統 (網路)	◆ Web 伺服器
◆ 防火牆	◆ 資料庫
◆ 作業系統	◆ 大型主機
◆ 規則監控	◆ 弱點評估系統
◆ 驗證	◆ 目錄服務
◆ 路由器與交換器	◆ 網路管理系統
◆ VPN	◆ 專屬系統

您可以使用標準 JavaScript 開發工具與 Collector SDK 來撰寫 JavaScript 收集器。

1.5.2 連接器與整合器

連接器可透過標準通訊協定 (例如 JDBC 與 Syslog) 提供收集器管理員至事件來源的連接。事件會從 「連接器」傳至 「收集器」進行剖析。

整合器可讓補救行動在 Sentinel 以外的系統執行。例如，關連行動可以使用 SOAP Integrator 啓始化 Novell Identity Manager 工作流程。

選擇性的 「矯正 AR 整合器」可以從 Sentinel 事件建立矯正票證。如需詳細資訊，請參閱《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的「Action Manager and Integrator」(動作管理員與 Integrator)。

1.5.3 關連規則與行動

關連規則可辨識事件資料流中的重要模式。關連規則觸發時會啓始化關連動作，例如傳送電子郵件通知、啓動 iTRAC 工作流程或使用 Integrator 執行動作。如需詳細資訊，請參閱《*Sentinel Rapid Deployment User Guide*》(Sentinel Rapid Deployment 使用者指南) 中的「Correlation Tab」(關連索引標籤)。

1.5.4 報告

您可以使用 JasperReports，從 Sentinel Rapid Deployment Web 介面執行各種儀表板與操作報告。報告通常是透過 「解決方案套件」來發送。

1.5.5 iTRAC 工作流程

iTRAC 工作流程針對管理事件提供一致且可重複的程序。工作流程範本通常是透過 「解決方案套件」來發送。iTRAC 隨附了一組預設範本，您可對其進行修改以滿足您的要求。如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》(Sentinel Rapid Deployment 使用者指南) 中的 「iTRAC Workflows」(iTRAC 工作流程)。

1.5.6 解決方案套件

解決方案套件為相關 Sentinel 內容 (關連規則、動作、iTRAC 工作流程與報告等) 的套裝集。Novell 針對特定企業需求提供 「解決方案套件」，例如 「PCI-DSS 解決方案套件」，可以解決 《支付卡產業之資料安全標準》的法規遵循問題。Novell 還建立了收集器套件，其中包含以特定事件來源 (例如 Windows Active Directory) 為主的內容。如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》(Sentinel Rapid Deployment 使用者指南) 中的「Solution Packs」(解決方案套件)。

1.6 語言支援

我們提供下列語言版本的 Sentinel 元件：

- 捷克文
- 英文
- 法文
- 德文
- 義大利文
- 日文
- 荷蘭語
- 波蘭文
- 葡萄牙文
- 簡體中文
- 西班牙文
- 繁體中文

系統要求 2

為達到最佳效能和可靠性，您必須在核准的軟體與硬體 (如本章節中所列) 上安裝 Sentinel Rapid Deployment 元件。本章列出的要求已經過全面品質保證和認證。

2.1 支援的平台

表格 2-1 列出了 Novell 認證或支援的軟體與作業系統組合。通過認證的組合已經過 Novell Engineering 之完整測試套裝軟體的測試。預期支援的組合可完全發揮功能。

2.1.1 支援的作業系統

Novell 支援在本節所述的作業系統版本上執行 Sentinel Rapid Deployment。此外，Novell 也支援在安裝了微幅更新 (例如安全性修補程式或 HotFix) 的那些作業系統上執行。但是，如果系統所在平台安裝了大幅更新，則不支援在該系統上執行 Sentinel Rapid Deployment，除非這些更新已經過 Novell 的測試與認證。

Sentinel Rapid Deployment 伺服器元件包括通訊伺服器、關連引擎、資料存取服務 (DAS)、Web 伺服器以及 Advisor 資料訂閱服務。

Sentinel 用戶端應用程式包括 Sentinel 控制中心 (SCC)、Sentinel 資料管理員 (SDM) 及 Sentinel Solution Designer (SSD)。

收集器管理員有特定的平台要求。

表格 2-1 *受支援與已認證的作業系統*

平台	伺服器元件	Sentinel 用戶端應用程式	收集器管理員
SUSE Linux Enterprise Server (SLES) 11 SP1 (64 位元)	已認證	已認證	已認證
SUSE Linux Enterprise Server (SLES) 11 SP1 (32 位元)	不支援	支援	支援
SUSE Linux Enterprise Server (SLES) 10 SP3 (64 位元)	已認證	支援	支援
SUSE Linux Enterprise Server (SLES) 10 SP3 (32 位元)	支援	支援	支援
Windows Server 2008 R2 (64 位元)	不支援	已認證	已認證

平台	伺服器元件	Sentinel 用戶端應用程式	收集器管理員
Windows Server 2003 R2 (64 位元)	不支援	支援	支援
Windows Server 2003 R2 (32 位元)	不支援	支援	支援
Windows XP SP3 (32 位元)	不支援	支援	不支援
Windows Vista SP2 (32 位元)	不支援	支援	不支援
Windows 7	不支援	已認證	不支援

請遵循下列指南以達到最佳效能、穩定性及可靠性：

- 對於 SLES，Sentinel Rapid Deployment 伺服器機器的作業系統必須至少包含 SLES 的基礎伺服器及 X Window 元件。
- 對於 Sentinel Rapid Deployment 伺服器，請使用 ext3 檔案系統。如需檔案系統的詳細資訊，請參閱 《*Storage Administration Guide*》 (儲存管理指南) 中的 「Overview of File Systems in Linux」 (Linux 中的檔案系統綜覽) (http://www.novell.com/documentation/sles11/stor_admin/data/filesystems.html)。

附註：

- 在安裝了 Open Enterprise Server 的 SLES 上，Sentinel Rapid Deployment 不受支援。
- Sentinel 6.1 Rapid Deployment 伺服器的 32 位元展示版本使用 32 位元硬體與作業系統，供規模有限的展示與測試環境之用。簽訂了 Sentinel 6.1 Rapid Deployment 支援合約的客戶或合作夥伴可以獲得來自 Novell 技術支援對此平台的部分支援，以解決可能會在 64 位元線上平台上重現的問題。由於 32 位元硬體固有的限制，Novell 技術支援不會對 32 位元展示版本發生的效能或延展性問題提供疑難排解。線上環境中不支援 32 位元展示版本。

2.2 硬體要求

Sentinel Rapid Deployment 伺服器元件在 x86-64 (64 位元) 硬體上執行，但某些作業系統存在一些例外，如第 2.1.1 節 「支援的作業系統」 (第 17 頁) 中所述。Sentinel 經過認證可於 AMD Opteron 與 Intel Xeon 硬體執行。Itanium 伺服器不受支援。

本節包含一些有關 Sentinel 系統設計的一般硬體建議。設計建議是根據事件發生率範圍而提出。不過，此處的建議則是以下列假設為基礎：

- 事件發生率是每秒事件數 (EPS) 範圍中高的一端。
- 平均事件大小是 1 KB。
- 所有事件都儲存於資料庫 (也就是說，沒有會放下事件的篩選器)。
- 資料庫會儲存九十天的線上資料量。
- 表格 2-2 (第 19 頁) 及表格 2-3 (第 19 頁) 中的規格中不包含 Advisor 資料的儲存空間。
- Sentinel 伺服器提供預設的 5 GB 磁碟空間，用於儲存無法立即插入資料庫的暫時快取事件資料。
- 另外，Sentinel 伺服器也提供預設的 5 GB 磁碟空間，用於儲存無法立即插入至彙總事件檔案的事件。
- 選購的 Advisor 訂閱在伺服器則額外需要 1 GB 的磁碟空間。

Sentinel 實作的硬體建議因個人的實作而異，因此建議您先諮詢 Novell 諮詢服務或任意 Novell Sentinel 合作夥伴，再最終確定 Sentinel 架構。以下建議可做爲指南使用。

在 SLES 版本中，資料庫與 Sentinel Rapid Deployment 伺服器嵌入在一起，並與該伺服器安裝到同一部機器上。

附註：由於事件載入和本地快取動作的高度需求，Sentinel 伺服器需要至少具備 4 個磁碟轉軸的本地或共用等量磁碟陣列 (RAID)。

表格 2-2 *單機組態 (最大 2000 eps)*

配件	RAM	空白鍵	CPU
機器 1：Sentinel Rapid Deployment 伺服器 ◆ 內嵌式 PostgreSQL 資料庫 (3 GB) ◆ 收集器管理員 (1228 MB) ◆ DAS_Core (1579MB) ◆ DAS_Binary (1404MB) ◆ 關連引擎 (1073 MB) ◆ 4 個收集器 (Generic、Cisco、Snort 和 IBM，每個產生 500 eps) ◆ 已部署 10 個關連規則 ◆ 10 個唯一的 Active View ◆ 3 個並行使用者 ◆ 已部署 2 個映射	16 GB	1 TB，SAS (15K rpm) 硬碟 硬體 RAID 10	Dell PowerEdge 2900，2 x Quad-Core Intel Xeon E5310 (1.6 GHz)，以及 Gigabit 乙太網路 NIC

表格 2-3 *三部機器的組態 (最大 5000 eps)*

配件	RAM	空白鍵	CPU
機器 1：Sentinel Rapid Deployment 伺服器 ◆ 內嵌式 PostgreSQL 資料庫 (3 GB) ◆ 收集器管理員 (1228 MB) ◆ DAS_Core (1579MB) ◆ DAS_Binary (1404MB) ◆ 關連引擎 (1073 MB) ◆ 4 個收集器 (每個產生 500 eps，遠端收集器管理員 1 產生 1500 EPS，遠端收集器管理員 2 產生 1500 EPS。	16 GB	1 TB，SAS (15K rpm) 硬碟 硬體 RAID 10	Dell PowerEdge 2900，2 x Quad-Core Intel Xeon E5310 (1.6 GHz)，以及 Gigabit 乙太網路 NIC
電腦 2：收集器管理員 ◆ 收集器管理員 / 收集器 ◆ 3 個收集器 (每個產生 500 eps)	4 GB	300 GB，SATA (3 Gbit/s) 硬碟	Intel Core 2 Duo E6750 (2.66 GHz)，以及 Gigabit 乙太網路 NIC

配件	RAM	空白鍵	CPU
電腦 3：收集者管理員 ◆ 收集者管理員 / 收集者 ◆ 3 個收集器 (每個產生 500 eps)	4 GB	300 GB，SATA (3 Gbit/s) 硬碟	Intel Core 2 Duo E6750 (2.66 GHz)，以及 Gigabit 乙太網路 NIC

2.3 支援的網頁瀏覽器

- Mozilla Firefox 3.*x*
- Internet Explorer 8.*x*

2.4 虛擬環境

Sentinel Rapid Deployment 已在 VMWare ESX Server 上經過廣泛測試，並且 Novell 完全支援在此環境中執行 Sentinel Rapid Deployment。爲了在 ESX 上或任意其他虛擬環境中實現能與實體機器測試結果相媲美的效能結果，虛擬環境應根據建議的實體機器要求提供同樣的記憶體、CPU、磁碟空間及 I/O。

如需針對 SLES 系統之實體機器建議的相關資訊，請參閱第 2.2 節 「硬體要求」 (第 18 頁)。

2.5 建議的限制

本節所述的限制是以 Novell 或客戶已經執行的效能測試爲依據提出的建議，而並非絕對限制。這些建議限制只是些近似值。在高度動態的系統中，最好設定一些緩衝，以便爲系統擴展預留空間。

- 第 2.5.1 節 「收集器管理員限制」 (第 20 頁)
- 第 2.5.2 節 「報告限制」 (第 21 頁)

2.5.1 收集器管理員限制

除非另有指定，否則收集器管理員限制會假設系統符合如下要求： 4 個 CPU 核心，每個核心頻率爲 2.2 GHz，RAM 爲 4 GB，作業系統爲 SLES 11。

***表格 2-4** 收集器管理員效能數值*

屬性	限制	備註
最大收集器管理員數	20	此限制假設每個收集器管理員都以低 EPS (例如低於 100 EPS) 執行。此限制隨 EPS 的增大而變小。
單個收集器管理員上的連接器 (完全利用) 數上限	每個 CPU 核心 1 個，且至少保留 1 個 CPU 核心供作業系統和其他處理作業使用	完全利用的連接器是指以該類型的連接器所能實現的最高 EPS 執行的連接器。
單個收集器管理員上的收集器 (完全利用) 數上限	每個 CPU 核心 1 個，且至少保留 1 個 CPU 核心供作業系統和其他處理作業使用	完全利用的收集器是指以該類型的收集器所能實現的最高 EPS 執行的收集器。

屬性	限制	備註
單個收集器管理員上的設備數上限	2000	對於 Sentinel Rapid Deployment 伺服器來說，該限制也是 2000。因此如果某個收集器管理員上有 2000 個設備，則單是這個收集器管理員就會使 Sentinel 整個系統達到設備上限。
Sentinel Rapid Deployment 伺服器的設備數上限	2000	Sentinel Rapid Deployment 伺服器上的設備上限是 2000。

2.5.2 報告限制

表格 2-5 報告效能數值

屬性	限制	備註
儲存報表數上限	200	此限制可能隨報告大小及伺服器上未被系統的其餘元件使用的可用磁碟空間而增大或減小。
同時執行的最大報告數	3	該限制假設伺服器資源目前尚未被資料收集或其他任務高度佔用。

2.6 測試結果

Sentinel Rapid Deployment 可讓您根據環境的需求設定不同的組態。以下效能測試資訊是 Novell 針對下列各表中所列的特定組態進行的測試結果。

Sentinel 實作的硬體建議因各實作而異；因此建議您先諮詢 Novell 諮詢服務或任意 Novell Sentinel 合作夥伴，再最終確定 Sentinel 架構。以下測試資訊可做為指南使用。

Linux 測試的執行是為了調整不同數量的設備所能達到的最大 EPS 值，以及特定 EPS 值下所允許的最大設備數。使用了以下硬體組態：

- **CPU 核心數：** 4
- **CPU 型號：** Intel Xeon CPU X5770，2.93 GHz
- **RAM ：** 16 GB
- **硬碟大小 (+RAID 類型及 RAID 中的磁碟數) ：** 1.7 TB (RAID 5，6 個磁碟)

附註：所有測試皆是使用 syslog 型事件來源完成的。其他連接器可能提供不同的效能。

下表顯示了您在 SLES 系統上使用不同數量的設備可以調整的最大 EPS：

表格 2-6 SLES 系統上的最大 EPS

系統設定	設備	最大 EPS
4 個包含 10 個收集器的收集器管理員 (一個本地，三個遠端)，每個產生 500 EPS	25	5,000

系統設定	設備	最大 EPS
4 個包含 10 個收集器的收集器管理員 (一個本地，三個遠端)，每個產生 500 EPS	100	5,000
4 個包含 10 個收集器的收集器管理員 (一個本地，三個遠端)，每個產生 500 EPS	1,000	5,000

下表顯示了您在 SLES 系統上使用不同 EPS 率可調整的最大設備數：

表格 2-7 *SLES 系統上的最大設備數*

系統設定	EPS	最大設備數
1 個包含 1 個收集器的收集器管理員，產生 500 EPS	500	2,000
1 個包含 2 個收集器的收集器管理員，每個產生 500 EPS	1,000	2,000
1 個包含 3 個收集器的收集器管理員，每個產生 500 EPS	1,500	2,000

附註：

- 如果要調整更多 EPS 或設備，請安裝更多收集器管理員。
- 最大設備數限制並非絕對限制，而是以 Novell 已經執行的效能測試為依據提出的建議。該限制假設每部設備每秒的平均事件發生率很低 (低於 3 EPS)。較高的 EPS 率會導致可承受設備上限偏低。您可以使用公式 (設備上限) x (每部設備的平均 EPS) = 事件發生率上限，來得到特定平均 EPS 率或設備數的約略限制，只要設備數上限不超過上述限制即可。

安裝 3

本章節提供安裝 Sentinel Rapid Deployment 和用戶端元件的相關資訊。

3.1 綜覽

Sentinel 安裝套件爲您提供了單台機器的簡易伺服器安裝程式，可安裝執行 Sentinel Rapid Deployment 所需的所有元件。Sentinel Rapid Deployment 伺服器安裝程式會安裝下列元件：

3.1.1 伺服器元件

表格 3-1 Sentinel Server 元件與應用程式

元件	描述
	Sentinel 資料庫會儲存組態與事件資料。
訊息匯流排	JMS 型訊息匯流排會處理 Sentinel 系統各元件之間的通訊。
關連引擎	關連引擎會執行即時事件分析。
Advisor	Advisor 提供偵測到之 IDS 攻擊與弱點掃描輸出之間的即時關連，可讓您立即識別組織所面臨的驟增風險。
資料存取服務	包含資料儲存、查詢、顯示與處理元件。
Web 伺服器	支援 Sentinel Rapid Deployment 的 Web 介面。
收集器管理員	用於處理事件來源連線、資料剖析與映射等的服務。
	您可以使用 Sentinel Rapid Deployment Web 介面所提供的收集器管理員安裝程式，將收集器管理員配送至其他位置、其他機器及其他作業系統。例如，您可以在 Windows 機器上安裝額外的 「收集器管理員」以收集 Windows 事件。

元件	描述
iTRAC	Sentinel 提供 iTRAC 工作流程管理系統，以定義與自動化事件回應的程序。在 Sentinel 中利用關聯性規則或透過手動方式所識別的事件，都可以與 iTRAC 工作流程建立關聯。

3.1.2 用戶端應用程式

用戶端應用程式 (Sentinel 控制中心、Sentinel 資料管理員及 Solution Designer) 預設會安裝在 Sentinel Rapid Deployment 伺服器上。您可以使用以下任意一種方式啓動用戶端應用程式：

- 使用 Sentinel Rapid Deployment Web 介面。用戶端系統中應安裝 Java 1.6.0_20 或更新版本，並且 JRE 路徑應設定爲透過 Webstart 啓動 Sentinel 應用程式。

  請將 JAVA_HOME 環境變數設定爲指向 JRE 6 資料夾的位置。將輸出路徑設定爲指向 JRE 6 位置下的 bin 資料夾。
- 以擁有 Sentinel Rapid Deployment 安裝檔案之使用者的身分使用 < *安裝目錄* >/bin。例如：

  ```
  ./bin/<client_application>.sh
  ```

表格 3-2 Sentinel 用戶端應用程式

元件	描述
Sentinel 控制中心	適用於安全性或法規遵循分析師的主控台。
Sentinel 資料管理員	資料庫管理公用程式。
Solution Designer	用於建立解決方案套件的應用程式。
Sentinel 收集器管理員	用於處理事件來源連接、資料剖析與映射等的服務。收集器管理員安裝在 Sentinel 伺服器上，但使用可下載的安裝程式可在遠端 Windows 或 Linux 機器上安裝額外的收集器管理員。

3.2 在 SUSE Linux Enterprise Server 上安裝

3.2.1 必要條件

請在安裝 Sentinel Rapid Deployment 之前先確保您符合下面的先決條件。如需這些先決條件 (包括經過認證的平台清單) 的詳細資訊，請參閱第 2 章 「系統要求」 (第 17 頁)。

重要：使用完整安裝程式的 Sentinel Rapid Deployment 安裝應永遠在「乾淨的」系統上進行。如果您的任意一台機器上先前安裝了其他版本的 Sentinel，例如 Sentinel Classic 或 Sentinel Log Manager，您必須先將其解除安裝。如需解除安裝先前版本之 Sentinel 的相關資訊，請參閱相應的安裝指南：

- 若要解除安裝 Senitnel Classic，請參閱《Sentinel Installation Guide》(Sentinel 安裝指南) (http://www.novell.com/documentation/sentinel61/s61_install/?page=/documentation/sentinel61/s61_install/data/bgpq4la.html) 中的「Uninstalling Sentinel」(解除安裝 Sentinel) 一章。
- 若要解除安裝 Sentinel Log Manager，請參閱《Sentinel Log Manager 1.1 Installation Guide》(Sentinel Log Manager 1.1 安裝指南) (http://www.novell.com/documentation/novelllogmanager11/log_manager_install/?page=/documentation/novelllogmanager11/log_manager_install/data/bor9aaf.html) 中的「Uninstalling Sentinel Log Manager」(解除安裝 Sentinel Log Manager) 一章。

伺服器

- 確定每部伺服器機器都符合最低系統要求。如需系統要求的詳細資訊，請參閱第 2 章「系統要求」(第 17 頁)。
- 以 hostname -f 指令傳回有效主機名稱的方法設定作業系統。
- 若您想從 Sentinel 系統傳送郵件通知，請安裝並設定 SMTP 伺服器。

用戶端

- 確定每部用戶端機器都符合最低系統要求。如需這些先決條件的詳細資訊，請參閱第 2 章「系統要求」(第 17 頁)。
- 確定您從中執行安裝程式之目錄的名稱僅包含 ASCII 字元 (且不含特殊字元)。
- 當您在 Linux 機器上安裝遠端收集器管理員或用戶端應用程式時，請確定並沒有針對管理員使用者爲 /tmp 資料夾設定資料夾層級的限制。
- 請務必爲要在 Windows 上執行收集器管理員的網域使用者提供進階使用者權限，因爲一般的使用者權限無法進行收集器管理員安裝。
- 如果將收集器管理員安裝於 64 位元的機器上，請確定有 32 位元的程式庫可用。若執行以專屬連接器語言 (包括 2008 年 6 月前撰寫的所有「收集器」) 所撰寫的「收集器」，以及執行若干「連接器」(例如「LEA 連接器」) 時，就需要 32 位元的程式庫。Javascript 型的「收集器」與 Sentinel 的其他「收集器」皆可支援 64 位元。請驗證是否有這些程式庫可用，這對於 Linux 平台格外重要，此類平台預設可能未包含這些程式庫。

Advisor

若要安裝 Advisor，您必須購買 Sentinel 入侵偵測與 Advisor 資料訂閱。購買訂閱後，請使用您的 Novell eLogin 下載和更新 Advisor 資料。如需詳細資訊，請參閱《*Sentinel Rapid Deployment User Guide*》(Sentinel Rapid Deployment 使用者指南) 中的「Advisor Usage and Maintenance」(Advisor 的使用與維護) 一章。

3.2.2 安裝 Sentinel Rapid Deployment

您可以使用以下幾種方式安裝 Sentinel Rapid Deployment 伺服器：

- 「使用 Root 權限的單一程序檔安裝」 (第 26 頁)
- 「非 root 安裝」 (第 28 頁)

安裝期間，Sentinel Rapid Deployment 安裝程式程序檔會提供下列選項：

- **-all** ： 必須具備根使用者權限才能使用此選項。此選項會建立一個使用者 (預設值： novell)、使用者群組 (預設值： novell)，然後安裝 Sentinel Rapid Deployment 伺服器。它還會在系統啓動時自動執行 Sentinel Rapid Deployment 服務。
- **-install** ： 此選項僅會安裝 Sentinel Rapid Deployment 伺服器。
- **-createuser** ： 必須具備根使用者權限才能使用此選項。此選項僅會建立使用者 (預設值： novell) 和使用者群組 (預設值： novell)。
- **-createservice** ： 必須具備根使用者權限才能使用此選項。此選項僅提供在系統啓動時自動執行 Sentinel Rapid Deployment 服務的功能。
- **-help** ： 此選項會顯示如何使用安裝程序檔選項的相關說明。

使用 Root 權限的單一程序檔安裝

1 以 root 使用者的身分登入。

執行安裝的使用者必須對將用於存放下載之安裝程式檔案的暫存目錄具備寫入權限。

2 從 Novell 下載網站 (http://download.novell.com/) 將 sentinel6_rd_linux_x86-64.tar.gz 安裝程式下載至暫存目錄。

3 解壓縮安裝程式：

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4 移至解壓縮安裝程式的目錄：

```
cd sentinel6_rd_linux_x86-64
```

5 使用 -all 選項執行 install.sh 程序檔：

```
./install.sh -all
```

安裝程序檔會先檢查可用記憶體及磁碟空間。如果可用記憶體少於 1 GB，程序檔會自動終止安裝。如果可用記憶體大於 1 GB 但少於 4 GB，程序檔會顯示一則訊息，提示您記憶體少於建議的大小。另外還會詢問您是否要繼續安裝。若要繼續安裝，請輸入 y，若不想繼續，請輸入 n。

6 指定使用者名稱，或按 Enter 選取預設使用者名稱。預設使用者名稱爲 novell。

如果指定的使用者名稱已經存在，安裝程式會顯示一則訊息，提示您該使用者已存在，並列出使用者所在群組。繼續進行步驟 8。

如果指定的使用者名稱不存在，安裝程式會建立該使用者名稱。繼續進行步驟 7。

7 指定群組名稱，或按 Enter 選取預設群組名稱。預設群組名稱爲 novell。

如果指定的群組名稱已經存在，安裝程式會繼續安裝。如果指定的群組名稱不存在，安裝程式會建立該群組，並顯示一則訊息，通知您已在指定群組下建立指定的使用者名稱。

指定的使用者與群組將擁有 Sentinel 的安裝與執行中程序。

8 指定安裝路徑，或按 Enter 選取預設路徑。預設路徑爲 /opt/novell/。

指定的安裝路徑不得包含空格。如果包含空格，安裝程序檔會提示您提供不含空格的安裝路徑。

9 輸入對應的編號，選擇下列其中一種語言：

序號	語言
1	捷克文
2	英文
3	法文
4	德文
5	義大利文
6	日文
7	荷蘭語
8	波蘭文
9	葡萄牙文
10	簡體中文
11	西班牙文
12	繁體中文

使用者授權合約會以選取的語言顯示。

10 閱讀使用者授權合約，若您同意本授權合約而且要繼續安裝，請輸入 1。若要結束安裝，請輸入 2。

安裝程式便會開始解壓縮檔案，並提示您提供授權。

11 若要使用 90 天的試用授權金鑰，請輸入 1；若要使用有效的授權金鑰，請輸入 2。

如果您輸入 2，安裝程式會提示您輸入有效的 Sentinel RD 授權金鑰。如果您指定的授權金鑰無效，安裝程式會提示您重新指定有效的授權金鑰。如果第二次指定的授權金鑰仍無效，系統會自動安裝 90 天的試用授權金鑰。您可以稍後再輸入有效的授權。

程序檔隨即會載入試用授權或有效授權。

12 指定 dbauser 使用者的密碼，並再次指定以確認該密碼。

dbauser 身分證明是用來在 PostgreSQL 資料庫中建立資料表與分割區。

13 指定 admin 使用者的密碼，並再次指定以確認該密碼。

當系統提示您指定 admin 和 dbuser 使用者的密碼時，請勿在密碼中使用反斜線 (\) 與單引號 (‘) 字元，因爲 PostgreSQL 資料庫不允許使用這些字元。

安裝程序檔會安裝 PostgreSQL 資料庫，建立表格與分割區，然後安裝 Sentinel Rapid Deployment 伺服器。

安裝之後，您可以：

- 移至 https://< *伺服器 IP*>:8443/sentinel 以啓動 Sentinel Rapid Deployment Web 介面。< *伺服器 IP*> 是指安裝了 Sentinel Rapid Deployment 之機器的 IP 位址。
- 以步驟 6 中建立的使用者身分執行 < *安裝目錄* >/bin/control_center.sh，以啓動 Sentinel 控制中心。

非 root 安裝

如果組織規則禁止以根身分執行完整安裝程序，您可以使用兩個部分來完成安裝。安裝程序的第一個部分必須以根權限執行，而第二個部分可以使用 Sentinel 管理使用者 (在第一個部分所建立) 來執行。

1 登入要安裝 Sentinel Rapid Deployment 的伺服器。

   執行安裝的使用者必須對將用於存放下載之安裝程式檔案的暫存目錄具備寫入權限。

2 從 Novell 下載網站 (http://download.novell.com/) 將 sentinel6_rd_linux_x86-64.tar.gz 安裝程式下載至暫存目錄。

3 解壓縮安裝程式：

```
tar zxvf sentinel6_rd_linux_x86-64.tar.gz
```

4 以 root 使用者的身分登入。

5 移至解壓縮安裝程式的目錄：

```
cd sentinel6_rd_linux_x86-64
```

6 使用 -createuser 選項執行 install.sh 程序檔：

```
./install.sh -createuser
```

7 指定使用者名稱，或按 Enter 選取預設使用者名稱。預設使用者名稱為 novell。

   如果指定的使用者名稱已經存在，安裝程式會顯示一則訊息，提示您該使用者已存在，並列出使用者所在群組。繼續進行步驟 9。

   如果指定的使用者名稱不存在，安裝程式會建立該使用者名稱。繼續進行步驟 8。

8 指定群組名稱，或按 Enter 選取預設群組名稱。預設群組名稱為 novell。

   如果指定的群組名稱已經存在，安裝程式會繼續安裝。如果指定的群組名稱不存在，安裝程式會建立該群組，並顯示一則訊息，通知您已在指定群組下建立指定的使用者名稱。

   指定的使用者與群組將擁有 Sentinel 的安裝與執行中程序。

9 指定安裝路徑，或按 Enter 選取預設路徑。預設路徑為 /opt/novell/。

   指定的安裝路徑不得包含空格。如果包含空格，安裝程序檔會提示您提供不含空格的安裝路徑。

10 以非根使用者的身分登入。例如：

```
su - novell
```

11 使用 -install 選項執行安裝程序檔：

```
./install.sh -install
```

   安裝程序檔會先檢查可用記憶體及磁碟空間。如果可用記憶體少於 1 GB，程序檔會自動終止安裝。如果可用記憶體大於 1 GB 但少於 4 GB，程序檔會顯示一則訊息，提示您記憶體少於建議的大小。另外還會詢問您是否要繼續安裝。若要繼續安裝，請輸入 y，若不想繼續，請輸入 n。

12 指定安裝路徑，或按 Enter 選取預設路徑。預設路徑為 /opt/novell/。

   指定的安裝路徑不得包含空格。如果包含空格，安裝程序檔會提示您提供不含空格的安裝路徑。

13 輸入對應的編號，選擇下列其中一種語言：

序號	語言
1	捷克文
2	英文
3	法文
4	德文
5	義大利文
6	日文
7	荷蘭語
8	波蘭文
9	葡萄牙文
10	簡體中文
11	西班牙文
12	繁體中文

使用者授權合約會以選取的語言顯示。

14. 閱讀使用者授權合約，若您同意本授權合約而且要繼續安裝，請輸入 1。若要結束安裝，請輸入 2。

    安裝程式便會開始解壓縮檔案，並提示您提供授權。

15. 若要使用 90 天的試用授權金鑰，請輸入 1；若要使用有效的授權金鑰，請輸入 2。

    如果您輸入 2，安裝程式會提示您輸入有效的 Sentinel RD 授權金鑰。如果您指定的授權金鑰無效，安裝程式會提示您重新指定有效的授權金鑰。如果第二次指定的授權金鑰仍無效，系統會自動安裝 90 天的試用授權金鑰。您可以稍後再輸入有效的授權。

    程序檔隨即會載入試用授權或有效授權。

16. 指定 dbauser 使用者的密碼，並再次指定以確認該密碼。

    dbauser 身分證明是用來在 PostgreSQL 資料庫中建立資料表與分割區。

17. 指定 admin 使用者的密碼，並再次指定以確認該密碼。

    當系統提示您指定 admin 和 dbauser 使用者的密碼時，請勿在密碼中使用反斜線 (\) 與單引號 (‘) 字元，因為 PostgreSQL 資料庫不允許使用這些字元。

18. (視情況而定) 安裝完成後，如果您要在系統啟動時自動執行 Sentinel Rapid Deployment 服務，請使用 -createservice 選項以根使用者身分執行 install.sh 程序檔：

    ```
    ./install.sh -createservice
    ```

安裝之後，您可以：

- 移至 https://< *伺服器 IP*>:8443/sentinel 以啓動 Sentinel Rapid Deployment Web 介面。< *伺服器 IP*> 是指安裝了 Sentinel Rapid Deployment 之機器的 IP 位址。
- 以上述步驟 7 中建立的使用者身分執行 < *安裝目錄* >/bin/control_center.sh，以啓動 Sentinel 控制中心。

3.3 安裝收集器管理員和用戶端應用程式

使用 Novell Sentinel Rapid Deployment Web 介面來下載「收集器管理員」安裝程式與「用戶端」安裝程式。

- 第 3.3.1 節「下載安裝程式」(第 30 頁)
- 第 3.3.2 節「Sentinel Rapid Deployment 用戶端元件的連接埠號碼」(第 30 頁)
- 第 3.3.3 節「安裝 Sentinel 用戶端應用程式」(第 31 頁)
- 第 3.3.4 節「安裝 Sentinel 收集器管理員 (在 SLES 或 Windows 上)」(第 33 頁)

3.3.1 下載安裝程式

1 開啓網頁瀏覽器並瀏覽下列 URL：

```
https://<svrname.example.com>:8443/sentinel
```

將 <*svrname.example.com*> 取代爲正在執行 Sentinel 之伺服器的實際 DNS 名稱或 IP 位址。URL 有大小寫之分。

2 若系統提示您驗證證書，請檢閱證書資訊，如果證書資訊有效，請按一下 *「是」*。

3 指定使用者名稱與密碼以存取 Sentinel 帳戶。

4 使用 *「語言」*下拉式清單來選取語言。

此語言是和 Sentinel Rapid Deployment 伺服器及您本機電腦的語言代碼相同的語言。確定您瀏覽器的語言設定已設定爲支援想要的語言。

5 按一下 *「登入」*。

6 選取 *「應用程式」*。

您可以下載下列安裝程式：

選項	描述	動作
收集器管理員安裝程式	收集器管理員安裝程式可讓您在支援的 Windows 與 Linux 平台上安裝 Sentinel 收集器管理員。	按一下 *「下載收集器管理員安裝程式」*並依照畫面上的指示進行。
用戶端安裝程式	用戶端安裝程式可讓您在支援的平台上安裝 Sentinel 控制中心、Sentinel Solution Designer 與 Sentinel 資料管理員。	按一下 *「下載用戶端安裝程式」*並依照畫面上的指示進行。

如需安裝收集器管理員的詳細資訊，請參閱第 3.3.4 節「安裝 Sentinel 收集器管理員 (在 SLES 或 Windows 上)」(第 33 頁)；如需安裝用戶端安裝程式的相關資訊，請參閱第 3.3.3 節「安裝 Sentinel 用戶端應用程式」(第 31 頁)。

3.3.2 Sentinel Rapid Deployment 用戶端元件的連接埠號碼

使用下列連接埠可設定防火牆設定，以允許 Sentinel Rapid Deployment 伺服器與用戶端元件之間的存取。

表格 3-3 Sentinel Rapid Deployment 元件的相容連接埠號碼

埠號碼	描述
61616	遠端收集器管理員使用此連接埠號碼透過 ActiveMQ 連接到 Sentinel Rapid Deployment 伺服器。
10013	Sentinel 控制中心使用此連接埠號碼透過代理連接到 Sentinel Rapid Deployment 伺服器。
5432	Sentinel 資料管理員使用此連接埠號碼連接到 PostgreSQL 資料庫。
8443	Web 用戶端使用此連接埠號碼連接到 Sentinel Rapid Deployment 伺服器。

3.3.3 安裝 Sentinel 用戶端應用程式

您可以在 Linux 或 Windows 系統上安裝 Sentinel 用戶端應用程式。若要安裝用戶端應用程式：

1 瀏覽至您將用戶端安裝程式下載到其中的資料夾。

2 從該檔案解壓縮安裝程序檔：

平台	動作
Windows	解壓縮 client_installer.zip 檔案。 檔案會解壓縮到名為 disk1 的目錄。
Linux	以 root 權限執行下列指令： `unzip client_installer.zip` 檔案會解壓縮到名為 disk1 的目錄。

3 移至安裝目錄並開始安裝：

平台	動作
Windows	執行 disk1\setup.bat **附註：**在 Windows Vista 機器上，從滑鼠右鍵功能表選項使用 *「以系統管理員身分執行」*選項，以啓動命令提示字元。
Linux	◆ **GUI 模式：**< *安裝目錄* >/disk1/setup.sh ◆ **主控台模式：**< *安裝目錄* >/disk1/setup.sh –console

下方所列的步驟僅適用於 GUI 模式。

4 按一下向下箭頭並選取其中一個語言。

5 在「歡迎」畫面中，按一下 *「下一步」*。

6 閱讀並接受「使用者授權合約」。按一下 *「下一步」*。

7 接受預設的安裝目錄，或按一下 *「瀏覽」*指定安裝位置。按一下 *「下一步」*。

重要：您無法安裝到名稱中含有特殊字元或非 ASCII 字元的目錄。例如，當您在 Windows x86-64 上安裝 Sentinel Rapid Deployment 時，預設路徑為 C:\\Program Files (x86)。如果要繼續安裝，您必須變更此預設路徑以避免使用如 (x86) 中的括弧等特殊字元。

8 選取要安裝的 Sentinel 應用程式。

下列選項可供使用：

元件	描述
Sentinel 控制中心	適用於安全性或法規遵循分析師的主控台。
Sentinel 資料管理員 (SDM)	用於手動資料庫管理活動。
Solution Designer	協助您建立解決方案套件。

9 若選擇安裝 「Sentinel 控制中心」，安裝程式會提示您指定要分配給 「Sentinel 控制中心」的最大記憶體空間。請指定僅限 「Sentinel 控制中心」使用的最大 JVM 堆積大小 (MB)。

允許範圍是 64-1024 MB。

如果已安裝任何 Sentinel 應用程式，此選項將無法使用。

10 指定使用者名稱，或按 Enter 選取預設使用者名稱。預設使用者名稱是 esecadm。

這是擁有已安裝之 Sentinel 產品的使用者的使用者名稱。如果該使用者不存在，系統就會在指定的目錄中建立一個使用者及主目錄。

11 指定使用者主目錄，或按 Enter 選取預設目錄。預設目錄是 /export/home。

如果使用者名稱是 esecadm，則對應的主目錄是 /export/home/esecadm。

12 如果您已在步驟 10 中選取了預設使用者名稱，請指定以 esecadm 使用者身分登入之使用者的密碼。否則，請設定您已在步驟 10 中建立之使用者的密碼。

13 指定下列資訊：

- **訊息匯流排連接埠：**通訊伺服器所傾聽的連接埠。直接連接通訊伺服器的元件會使用此連接埠。預設連接埠號碼為 61616。
- **Sentinel 控制中心代理連接埠：**SSL 代理伺服器 (資料存取伺服器代理) 所監聽以接受使用者名稱與密碼的連接埠。SSL 代理伺服器會根據已驗證的連接接受身分證明。「Sentinel 控制中心」會使用此連接埠來連接到 Sentinel 伺服器。預設連接埠號碼為 10013。
- **通訊伺服器主機名稱：**已安裝 Sentinel Rapid Deployment 伺服器之機器的機器 IP 位址或主機名稱。

請確定連接埠號碼與 Sentinel Rapid Deployment 伺服器上 < *安裝目錄* >/config/configuration.xml 中的連接埠號碼相同，才能進行通訊。請寫下這些連接埠，以便未來在其他機器安裝時使用。如需連接埠號碼的詳細資訊，請參閱第 3.3.2 節 「Sentinel Rapid Deployment 用戶端元件的連接埠號碼」 (第 30 頁)。

14 按 *「下一步」*。

隨即顯示安裝摘要。

15 按一下 *「安裝」*。

16 按一下 *「完成」*以完成安裝。

附註：再次登入時，請使用您在步驟 10 指定的使用者名稱。

如果忘記您設定的使用者名稱，請以根使用者身分開啓終端機主控台，然後輸入下列指令：

```
env | grep ESEC_USER
```

此指令會傳回使用者名稱 (若已建立該使用者)，以及已設定的環境變數。

3.3.4 安裝 Sentinel 收集器管理員 (在 SLES 或 Windows 上)

您可以從 Sentinel Rapid Deployment Web 介面中的 「應用程式」頁面下載 Sentinel 收集器管理員安裝程式。若要安裝收集器管理員：

1 瀏覽至已將收集器管理員安裝程式下載到其中的資料夾。

2 從該檔案解壓縮安裝程序檔：

平台	動作
Windows	解壓縮 scm_installer.zip 檔案。 檔案會解壓縮到名爲 disk1 的目錄。
Linux	以 root 權限執行下列指令： `unzip scm_installer.zip` 檔案會解壓縮到名爲 disk1 的目錄。

3 移至 disk1 目錄並開始安裝：

平台	動作
Windows	執行以下指令： `disk1\setup.bat`
Linux	◆ **GUI 模式：**< *安裝目錄* >/disk1/setup.sh ◆ **主控台模式：**< *安裝目錄* >/disk1/setup.sh –console

4 選取一種語言以繼續安裝。

5 閱讀 「歡迎」畫面，然後按一下 *「下一步」*。

6 閱讀並接受 「使用者授權合約」。按一下 *「下一步」*。

7 接受預設的安裝目錄，或按一下 *「瀏覽」*指定安裝位置，然後按一下 *「下一步」*。

重要：您無法安裝到名稱中含有特殊字元或非 ASCII 字元的目錄。例如，在 Windows x86-64 上安裝 Sentinel 時，預設路徑是 C:\\Program Files (x86)。如果要繼續安裝，您必須變更預設路徑以避免使用如 (x86) 中的括弧等特殊字元。

8 指定 「Sentinel 管理員」使用者名稱，以及對應之主目錄的路徑。

若已安裝任何 Sentinel 應用程式，此選項將無法使用。

- **OS Sentinel 管理員使用者名稱：**預設値是 esecadm。

  這是擁有已安裝之 Sentinel 產品的使用者的使用者名稱。如果該使用者不存在，系統就會建立一個使用者，並在指定的目錄建立對應的主目錄。

- **OS Sentinel 管理員使用者主目錄：**預設是 /export/home。如果使用者名稱是 esecadm，則對應的主目錄是 /export/home/esecadm。

若要以 esecadm 使用者身分登入，您必須先設定其密碼。

9 指定下列資訊：

- **訊息匯流排連接埠：**通訊伺服器所傾聽的連接埠。直接連接通訊伺服器的元件會使用此連接埠。預設連接埠號碼為 61616。
- **通訊伺服器主機名稱：**已安裝 Sentinel Rapid Deployment 伺服器之機器的機器 IP 或主機名稱。

確定連接埠號碼與 Sentinel 系統中的每部機器相同，才能進行通訊。請寫下這些連接埠，以便未來在其他機器安裝時使用。

10 按 *「下一步」*。

11 指定下列資訊：

- **自動記憶體組態：**選取要配置給 「收集器管理員」的記憶體總數。安裝程式會自動決定在各元件間分配記憶體的最佳方式，同時將預估的作業系統與資料庫負擔納入考量。

重要：您可以修改 configuration.xml 檔案中的 -Xmx 值，以變更配置給收集器管理員程序的 RAM。configuration.xml 檔案位於 < *安裝目錄* >/config (Linux) 或 < *安裝目錄* >\config (Windows)。

- **自定記憶體組態：**按一下 *「設定組態」*以微調記憶體配置。機器上的記憶體充足時，此選項才可用。

12 按 *「下一步」*。

系統會顯示摘要畫面，其中包含您選擇要安裝的功能。

13 按一下 *「安裝」*。

14 安裝完成之後，系統會提示您輸入 ActiveMQ JMS 策略用來連接到仲介的使用者名稱與密碼。

使用使用者名稱 collectormanager 及其對應的密碼，該密碼可在 Sentinel 伺服器上的 < *安裝目錄* >/config/activemqusers.properties 檔案中找到。

activemqusers.properties 檔案中提供的身分證明範例如下：

```
collectormanager=cefc76062c58e2835aa3d777778f9295
```

collectormanager 是使用者名稱，cefc76062c58e2835aa3d777778f9295 是其對應的密碼。

安裝 「收集器管理員」服務時，必須使用 collectormanager 使用者與其對應的密碼。在此案例中，collectormanager 使用者只擁有執行 「收集器管理員」作業之通訊通道的必要存取權。

安裝完成之後，系統會提示您重新開機或再次登入，然後再手動啓動 Sentinel 服務。

15 按一下 *「完成」*重新啓動系統。

16 使用步驟 8 中指定的使用者名稱再次登入。

如果忘記了使用者名稱，請以根身分證明開啓終端機主控台，然後輸入下列指令。

```
env | grep ESEC_USER
```

此指令會傳回使用者名稱 (若已建立該使用者)，以及已設定的環境變數。

附註：在 Windows 2008 平台上安裝收集器管理員以及影像的收集器管理員時，出現一些問題。如需對這些問題進行疑難排解的相關資訊，請參閱附錄 B「疑難排解秘訣」(第 81 頁)。

3.4 手動啓動和停止 Sentinel 服務

若要手動啓動 Sentinel 服務，請使用以下任一指令：

平台	指令
Linux	<*install_directory*>/bin/sentinel.sh start
Windows	<*install_directory*>/bin/sentinel.bat start

若要手動停止 Sentinel 服務，請使用以下任一指令：

平台	指令
Linux	<*install_directory*>/bin/sentinel.sh stop
Windows	<*install_directory*>/bin/sentinel.bat stop

您還可以使用以下指令啓動或停止 Sentinel 服務。

```
/etc/init.d/sentinel.sh stop|start
```

3.5 手動升級 Java

Java 1.6.0_24 版與 Sentinel Rapid Deployment 伺服器安裝程式搭售，安裝 Sentinel Rapid Deployment 伺服器會同時安裝該 Java。不過，如果在伺服器上將 Java 升級到最新版本，則需要執行以下步驟，以便 Sentinel Rapid Deployment 使用最新版本。

1. 根據安裝了 Sentinel Rapid Deployment 伺服器的作業系統下載 jre 套裝軟體。

   執行升級的使用者必須對 Sentinel Rapid Deployment 安裝目錄及將用於存放下載之升級檔案的目錄具備寫入權限。

   - 如果在 SUSE Linux Enterprise Server 上安裝 Sentinel Rapid Deployment，請從 Java 下載網站 (http://www.java.com/en/download/manual.jsp) 下載 32 位元和 64 位元的 jre 套裝軟體。

2. 將 Sentinel Rapid Deployment 安裝目錄中的 jre 與 jre64 資料夾分別重新命名爲 jre_old 與 jre64_old。

   ```
   cd <install_path>/sentinel_rd
   mv jre jre_old
   mv jre64 jre64_old
   ```

   附註：如果 Java 升級無法正常運作，則需要重新命名以轉換爲舊版本。如果 Java 在升級後能夠正常運作，則可以刪除重新命名的資料夾。

3. 解壓縮下載的 jre 套裝軟體。
4. 將 32 位元資料夾與 64 位元目錄分別重新命名爲 jre 與 jre64。

5 將重新命名的 jre 與 jre64 資料夾複製到 Sentinel Rapid Deployment 的安裝目錄。

```
copy jre <install_path>/sentinel_rd/
copy jre64 <install_path>/sentinel_rd/
```

6 (視情況而定) 請確保為執行 Sentinel Rapid Deployment 伺服器的使用者設定了 jre 與 jre64 資料夾的必要擁有權與許可。

7 重新啓動 Sentinel Rapid Deployment 伺服器與瀏覽器，並檢查 Java 是否已正確安裝。

3.6 安裝後的組態

本節可協助您瞭解 Sentinel Rapid Deployment 服務的安裝後組態。

3.6.1 變更日期與時間設定

Sentinel 控制中心中的預設日期與時間格式可以覆寫。如需自定日期與時間格式以符合您當地時區的詳細資訊，請造訪 Java 網站 (http://java.sun.com/j2se/1.6.0/docs/api/java/text/SimpleDateFormat.html)。

1 編輯 SentinelPreferences.properties 檔案。

```
<install_directory>/config/SentinelPreferences.properties
```

2 移除下列行中的備註，並對 Sentinel 控制中心的事件日期 / 時間欄位自定日期與時間格式：

```
com.eSecurity.Sentinel.event.datetimeformat=yyyy-MM-dd'T'HH:mm:ss.SSSZ
```

3.6.2 設定 SMTP Integrator 以傳送 Sentinel 通知

在 Sentinel Rapid Deployment 中，JavaScript SendEmail 動作與 SMTP Integrator 搭配使用，可從 Sentinel 介面的各種環境中將郵件訊息傳送給郵件收件人。SMTP Integrator 必須使用有效的連線資訊進行設定才能正常工作。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Sending an E-mail」(傳送電子郵件)。

在每次 Sentinel 安裝中，都會自動建立 SendEmail 動作外掛程式的單一動作例項。除了在動作參數中設定郵件訊息的收件人及訊息內容之外，SendEmail 動作無需設定其他組態。

在下列情況中，Sentinel 會從內部觸發此 SendEmail 動作以傳送郵件：

- 產生關連規則時，即會觸發 SendEmail 動作。此 SendEmail 動作是以齒輪圖示表示的動作，僅對關連有效 (跟以 JS JavaScript 圖示表示的 JavaScript SendEmail 動作相反)。
- 工作流程包括設定為傳送電子郵件的郵件步驟或活動時。
- 使用者開啓事件並加以選取以執行設定為傳送電子郵件的活動時。
- 使用者在事件上按一下滑鼠右鍵並選取 *「電子郵件」*時。
- 使用者開啓事件並選取 *「電子郵件事件」*時。

3.6.3 收集器管理員服務

- 「安裝其他收集器管理員」 (第 37 頁)
- 「使用一般收集器」 (第 37 頁)

安裝其他收集器管理員

收集器管理員可管理所有資料收集程序與資料剖析。有時候，可能必須新增額外的「Sentinel 收集器管理員」節點至 Sentinel 環境，才能在各機器間達成負載平衡。遠端收集器管理員提供數種優點：

- 提供分散事件剖析與處理作業，可提高系統效能。
- 透過與事件來源並存，可在來源系統上進行過濾、加密和資料壓縮。這可降低網路頻寬要求，並對資料提供額外保護。
- 可在其他作業系統上安裝。例如，可在 Microsoft Windows 上安裝收集器管理員節點，以使用 WMI 通訊協定進行資料收集。
- 提供檔案快取功能，讓遠端收集器管理員可以在伺服器暫時忙著歸檔或處理突增事件時快取大量資料。這對於本身不支援事件快取的通訊協定 (例如，Syslog) 是一項優點。

在額外的機器上安裝 「收集器管理員」元件的例項，這些元件即可達成負載平衡。您可以在新機器上執行安裝程式，來安裝其他收集器管理員。如需安裝收集器管理員的詳細資訊，請參閱第 3.3.4 節 「安裝 Sentinel 收集器管理員 (在 SLES 或 Windows 上)」 (第 33 頁)。

使用一般收集器

安裝 Sentinel Rapid Deployment 伺服器期間，會設定名為 「一般收集器」的收集器。根據預設值，它會以每秒 5 個事件 (eps) 的速率建立事件。

如果要為系統配備任何其他收集器，您可以從 Novell 網站 (http://support.novell.com/products/sentinel/collectors.html) 下載。

3.6.4 管理時間

您必須將 Sentinel 伺服器連接到 NTP (網路時間通訊協定) 伺服器或其他類型的時間伺服器。若各機器上的系統時間不同步，則 「Sentinel 關連引擎」與 Active View 無法正常運作。系統不會將 「收集器管理員」傳來的事件視為即時事件，因此不會將這些事件直接傳送至「Sentinel 資料庫」，略過 「Sentinel 控制中心」與 「關連引擎」。

依預設，即時資料的限定值為 120 秒。您只要變更 event-router.properties 檔案中 esecurity.router.event.realtime.expiration 的值，即可完成修改。Sentinel 事件時間會根據 「信任裝置時間」或 「收集器管理員時間」填入。您可在設定收集器時，選取 「信任裝置時間」。「信任裝置時間」為裝置產生記錄的時間，「收集器管理員時間」則為 「收集器管理員系統」的本機系統時間。

3.7 LDAP 驗證

除了資料庫驗證之外，Sentinel Rapid Deployment 還支援 ·LDAP 驗證。您可以將 Sentinel Rapid Deployment 伺服器設定為使用 LDAP 驗證，讓使用者使用其 Novell eDirectory 或 Microsoft Active Directory 身分證明登入 Sentinel Rapid Deployment。

- 第 3.7.1 節 「綜覽」 (第 38 頁)

3.7.1 綜覽

您可以將 Sentinel Rapid Deployment 伺服器設定爲透過安全 SSL 連線進行 LDAP 驗證，既可對 LDAP 目錄使用匿名搜尋，也可以不使用。

附註：如果 LDAP 目錄已停用匿名搜尋，則不能將 Sentinel Rapid Deployment 伺服器設定爲使用匿名搜尋。

- **匿名搜尋：** 在建立 Sentinel Rapid Deployment LDAP 使用者帳戶時，您必須指定目錄使用者名稱，但無需指定使用者可辨識名稱 (DN)。

  當 LDAP 使用者登入 Sentinel Rapid Deployment 時，Sentinel Rapid Deployment 伺服器會根據指定的使用者名稱對 LDAP 目錄執行匿名搜尋，尋找對應的 DN，然後使用該 DN 對 LDAP 目錄驗證使用者登入。
- **非匿名搜尋：** 在建立 Sentinel Rapid Deployment LDAP 使用者帳戶時，您必須同時指定目錄使用者名稱與使用者 DN。

  當 LDAP 使用者登入 Sentinel Rapid Deployment 時，Sentinel Rapid Deployment 伺服器會使用指定的使用者 DN 對 LDAP 目錄驗證使用者登入，但不會對 LDAP 目錄執行任何匿名搜尋。

  此外，還有一種僅適用於 Active Directory 的方法。如需詳細資訊，請參閱使用 Active Directory 中的 UserPrincipalName 屬性進行非匿名 LDAP 驗證。

3.7.2 必要條件

輸出 LDAP 伺服器 CA 證書

與 LDAP 伺服器之間的安全 SSL 連線需要 LDAP 伺服器 CA 證書，您必須將該證書輸出爲以 Base64 編碼的檔案。

- **eDirectory** ： 請參閱「Exporting an Organizational CA's Self-Signed Certificate」(輸出組織 CA 自行簽署的證書) (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/a7elxuq.html)。

  若要輸出 iManager 中的 eDirectory CA 證書，必須安裝適用於 iManager 的 Novell Certificate Server 外掛程式。
- **Active Directory** ： 請參閱「如何啓用透過 SSL 的 LDAP 與協力廠商憑證授權單位」(http://support.microsoft.com/kb/321051)。

對 LDAP 目錄啓用匿名搜尋

若要使用匿名搜尋執行 LDAP 驗證，您必須對 LDAP 目錄啓用匿名搜尋。依預設，eDirectory 中會啓用匿名搜尋，而 Active Directory 中會停用。

若要對 LDAP 目錄啓用匿名搜尋，請參閱以下內容：

- **eDirectory** ： 請參閱 「Attributes on the LDAP Server Object」 (LDAP 伺服器物件屬性) (http://www.novell.com/documentation/edir88/edir88/?page=/documentation/edir88/edir88/data/agq8auc.html) 一節中的 ldapBindRestrictions。
- **Active Directory** ： ANONYMOUS LOGON 使用者物件必須擁有適當的清單許可以及對 sAMAccountName 與 objectclass 屬性的讀取權限。如需詳細資訊，請參閱 「如何設定為允許匿名查詢的 Active Directory」(http://support.microsoft.com/kb/320528)。

  對於 Windows Server 2003，您必須執行額外的組態設定。如需詳細資訊，請參閱「Configuring Active Directory on Windows Server 2003」(在 Windows Server 2003 上設定 Active Directory) (http://support.microsoft.com/kb/326690/en-us)。

3.7.3 設定 Sentinel 伺服器進行 LDAP 驗證

1. 確定您符合第 3.7.2 節 「必要條件」 (第 38 頁) 中所述的先決條件。
2. 以根使用者的身分登入 Sentinel Rapid Deployment 伺服器。
3. 將輸出的 LDAP 伺服器 CA 證書檔案複製到 < *安裝目錄* >/config 目錄。
4. 以下列方式設定證書檔案的擁有權和許可：

   chown novell:novell < *安裝目錄* >/config/< 證書檔案 >

   chmod 700 < *安裝目錄* >/config/< *證書檔案* >
5. 切換至 novell 使用者：

   ```
   su - novell
   ```
6. 移至 < *安裝目錄* >/bin 目錄。
7. 執行 LDAP 驗證組態程序檔：

   ./ldap_auth_config.sh

   程序檔會先將 config 目錄中的 auth.login 與 configuration.xml 組態檔案分別備份為 auth.login.sav 與 configuration.xml.sav，然後再對這兩份檔案進行修改以進行 LDAP 驗證。
8. 指定下列資訊：

   按 Enter 接受預設值，或指定一個新值以覆寫預設值。

   - **Sentinel 安裝位置**： Sentinel 伺服器上的安裝目錄。
   - **LDAP 伺服器的主機名稱或 IP 位址**： 安裝 LDAP 伺服器之機器的主機名稱或 IP 位址。預設值為 localhost。但是，您不應該在與 Sentinel 伺服器相同的機器上安裝 LDAP 伺服器。
   - **LDAP 伺服器連接埠**： 安全 LDAP 連線的連接埠號碼。預設連接埠號碼為 636。
   - **LDAP 目錄匿名搜尋**： 指定 y 以執行匿名搜尋。若不執行，請指定 n。預設值為 y。

     如果指定 n，請完成 LDAP 組態並執行 「不執行匿名搜尋的 LDAP 驗證」 (第 40 頁) 一節中所述的步驟。

* **使用的 LDAP 目錄：** 此參數僅在您已指定 「y」進行匿名搜尋時才會顯示。指定 1 以使用 Novell eDirectory，指定 2 以使用 Active Directory。預設値爲 1。
* **要在其中搜尋使用者的 LDAP 子樹狀結構：** 此參數僅在您已指定 「y」進行匿名搜尋時才會顯示。該子樹狀結構即使用者物件所在目錄中的子樹狀結構。以下分別是在 eDirectory 和 Active Directory 中指定子樹狀結構的範例：
  * eDirectory ：

    ```
    ou=users,o=novell
    ```

    附註：對於 eDirectory，如果未指定子樹狀結構，則會在整個目錄中執行搜尋。
  * Active Directory ：

    ```
    CN=users,DC=TESTAD,DC=provo, DC=novell,DC=com
    ```

    附註：對於 Active Directory，子樹狀結構不能爲空。
* **LDAP 伺服器證書的檔名：** 您已於步驟 3 中複製之 eDirectory/Active Directory CA 證書的檔名。

9 輸入下列値之一：

* y 以接受輸入的値
* n 以輸入新値
* q 以結束組態設定

組態成功設定後：

* LDAP 伺服器證書會新增到位於 < *安裝目錄* >/config/ldap_server.keystore 的 Keystore 中。
* < *安裝目錄* >/config 目錄中的組態檔案 auth.login 與 configuration.xml 會進行更新，以啓用 LDAP 驗證。

10 輸入 y 以重新啓動 Sentinel 服務。

重要：如果出現任何錯誤，請回復對 config 目錄中組態檔案 auth.login 與 configuration.xml 所做的變更：

```
cp -p auth.login.sav auth.login
cp -p configuration.xml.sav configuration.xml
```

11 (視情況而定) 如果對 LDAP 目錄匿名搜尋：指定了 n，請繼續 「不執行匿名搜尋的 LDAP 驗證」 (第 40 頁)。

不執行匿名搜尋的 LDAP 驗證

在設定 Sentinel Rapid Deployment 以進行 LDAP 驗證時，如果對 LDAP 目錄匿名搜尋指定了 n，則 LDAP 驗證不會執行匿名搜尋。

當您使用 Sentinel 控制中心建立 LDAP 使用者帳戶時，請務必爲非匿名 LDAP 驗證指定「*LDAP 使用者 DN*」。您可以對 eDirectory 與 Active Directory 使用此方法。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Creating an LDAP User Account for Sentinel」(爲 Sentinel 建立 LDAP 使用者帳戶)。

此外，對於 Active Directory，還有一種替代方法可以執行無需匿名搜尋的 LDAP 驗證。如需詳細資訊，請參閱使用 Active Directory 中的 UserPrincipalName 屬性進行非匿名 LDAP 驗證。

使用 Active Directory 中的 UserPrincipalName 屬性進行非匿名 LDAP 驗證

對於 Active Directory，您還可以使用 userPrinicipalName 屬性執行無需匿名搜尋的 LDAP 驗證：

1 確定已對 Active Directory 使用者將 userPrinicipalName 屬性設定爲 <*sAMAccountName@domain*>。

   如需詳細資訊，請參閱 「User-Principal-Name Attribute」 (User-Principal-Name 屬性) (http://msdn.microsoft.com/en-us/library/ms680857(VS.85).aspx)。

2 確定您已執行步驟 1 (第 39 頁) 至步驟 10 (第 40 頁)，並爲 「LDAP 目錄匿名搜尋：」 (第 39 頁) 指定了 n。

3 在 Sentinel 伺服器上，編輯 < *安裝目錄* >/config/auth.login 檔案中的 LdapLogin 區段：

```
LdapLogin {
 com.sun.security.auth.module.LdapLoginModule required
 userProvider="ldap://LDAP server IP:636/DN of the Container that contains
the user objects"
 authIdentity="{USERNAME}@Domain Name"
 userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
 useSSL=true;
 };
```

   例如：

```
LdapLogin {
 com.sun.security.auth.module.LdapLoginModule required
 userProvider="ldap://137.65.151.12:636/DC=Test-
AD,DC=provo,DC=novell,DC=com"
 authIdentity="{USERNAME}@Test-AD.provo.novell.com"
 userFilter="(&(sAMAccountName={USERNAME})(objectclass=user))"
 useSSL=true;
 };
```

4 重新啓動 Sentinel 服務：

```
/etc/init.d/sentinel stop
/etc/init.d/sentinel start
```

3.7.4 設定多個 LDAP 伺服器進行容錯移轉

若要將一或多個 LDAP 伺服器設定爲 LDAP 驗證的容錯移轉伺服器：

1 確定您已經完成步驟 2 (第 39 頁) 至步驟 10 (第 40 頁)，將 Sentinel 伺服器設定爲針對 LDAP 主要伺服器進行 LDAP 驗證。

2 以 novell 使用者身分登入 Sentinel 伺服器。

3 停止 Sentinel 服務。

```
/etc/init.d/sentinel stop
```

4 移至 < *安裝目錄* >/config 目錄：

```
cd <install_directory>/config
```

5 開啓 auth.login 檔案進行編輯。

```
vi auth.login
```

6. 更新 LdapLogin 區段中的 userProvider，以指定多個 LDAP URL。使用空格分隔各個 URL。

   例如：

   ```
   userProvider="ldap://ldap-url1 ldap://ldap-url2"
   ```

   對於 Active Directory，請確定 LDAP URL 中的子樹狀結構不為空。

   如需指定多個 LDAP URL 的詳細資訊，請參閱「Class LdapLogin Module」(LdapLogin 類別模組) (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) 中 userProvider 選項的描述。

7. 儲存變更。

8. 輸出各 LDAP 容錯移轉伺服器的證書，並將證書檔案複製到 Sentinel 伺服器上的 < *安裝目錄* >/config 目錄中。

   如需詳細資訊，請參閱「輸出 LDAP 伺服器 CA 證書」(第 38 頁)。

9. 確定您為各 LDAP 容錯移轉伺服器的證書檔案都設定了必要的擁有權和許可。

   ```
   chown novell:novell <install_directory>/config/<cert-file>
   ```

   ```
   chmod 700 <install_directory>/config/<cert-file>
   ```

10. 將各 LDAP 容錯移轉伺服器證書新增至「設定 Sentinel 伺服器進行 LDAP 驗證」(第 39 頁) 一節之步驟 8 中建立的 ldap_server.keystore。

    ```
    <install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
    -file <certificate-file> -alias <alias_name> -keystore
    ldap_server.keystore -storepass sentinel
    ```

    以 Base64 編碼格式的 LDAP 證書檔名取代 *<certificate-file>*，並以要輸入的證書別名取代 *<alias_name>*。

    重要：請確定您指定了別名。如果未指定別名，Keytool 預設會將 mykey 用作別名。將多個證書輸入至 Keystore 而未指定別名時，Keytool 會報告一個錯誤，指出該別名已經存在。

    ---

11. 啟動 Sentinel 服務。

    ```
    /etc/init.d/sentinel start
    ```

如果 Sentinel 伺服器在發現 LDAP 主要伺服器關閉之前就已逾時，則該服務可能無法連接到 LDAP 容錯移轉伺服器。若要確保 Sentinel 伺服器可連接到 LDAP 容錯移轉伺服器而不發生逾時：

1. 以根使用者身分登入 Sentinel 伺服器。
2. 開啟 sysct1.conf 檔案進行編輯：

   ```
   vi /etc/sysctl.conf
   ```

3. 確定 net.ipv4.tcp_syn_retries 值已設定為 3。如果該項目不存在，請予以新增。儲存檔案：

   ```
   net.ipv4.tcp_syn_retries = 3
   ```

4. 執行以下指令以使所做變更生效：

   ```
   /sbin/sysctl -p
   ```

   ```
   /sbin/sysctl -w net.ipv4.route.flush=1
   ```

5. 在 < *安裝目錄* >/bin 目錄的 control_center.sh 與 solution_designer.sh 中新增參數 -Desecurity.remote.timeout=60，以設定 Sentinel 伺服器逾時值：

control_center.sh ：

```
"<install_directory>/jre/bin/java" $MEMORY -
Dcom.esecurity.configurationfile=$ESEC_CONF_FILE -
Desecurity.cache.directory="<install_directory>/data/
control_center.cache" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
control_center_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -
Dice.pilots.html4.baseFontFamily="Arial Unicode MS" -
Desecurity.remote.timeout=60 -jar ../lib/console.jar
```

solution_designer.sh ：

```
"<install_directory>/jre/bin/java" -classpath $LOCAL_CLASSPATH $MEMORY -
Dcom.esecurity.configurationfile="$ESEC_CONF_FILE" -
Dsentinel.installer.jar.location="<install_directory>/lib/
contentinstaller.jar" -Desecurity.communication.service="sentinel_client"
-Dfile.encoding=UTF8 -Desecurity.dataobjects.config.file="/xml/
BaseMetaData.xml,/xml/WorkflowMetaData.xml,/xml/ActMetaData.xml" -
Djava.util.logging.config.file="<install_directory>/config/
solution_designer_log.prop" -
Djava.security.auth.login.config="<install_directory>/config/auth.login"
$SENTINEL_LANG_PROP $SENTINEL_CTRY_PROP -Desecurity.cache.directory=../
data/solution_designer.cache -Desecurity.remote.timeout=60
com.esecurity.content.exportUI.ContentPackBuilder
```

3.7.5 爲多個 Active Directory 網域設定 LDAP 驗證

如果要驗證的 LDAP 使用者處於多個 Active Directory 網域中，您可以採用下列方式將 Sentinel Rapid Deployment 伺服器設定爲使用 LDAP 驗證：

1. 確定您已經完成步驟 2 (第 39 頁) 至步驟 10 (第 40 頁)，將 Sentinel 伺服器設定爲針對第一個網域的 Active Directory 領域控制器進行 LDAP 驗證。同時確定爲「LDAP 目錄匿名搜尋：」 (第 39 頁) 指定了 n。
2. 以 novell 使用者身分登入 Sentinel 伺服器。
3. 停止 Sentinel 服務。

   ```
   /etc/init.d/sentinel stop
   ```
4. 移至 <*安裝目錄*>/config 目錄：

   ```
   cd <install_directory>/config
   ```
5. 開啓 auth.login 檔案進行編輯。

   ```
   vi auth.login
   ```
6. 編輯 LdapLogin 區段以指定多個 LDAP URL，以空格分隔各個 URL。

   例如：

```
LdapLogin {
        com.sun.security.auth.module.LdapLoginModule required
        userProvider="ldap://<IP of the domain 1 domain controller>:636
ldap://<IP of the domain 2 domain controller>:636"
        authIdentity="{USERNAME}"
        useSSL=true;
};
```

如需指定多個 LDAP URL 的詳細資訊，請參閱「Class LdapLogin Module」(LdapLogin 類別模組) (http://java.sun.com/javase/6/docs/jre/api/security/jaas/spec/com/sun/security/auth/module/LdapLoginModule.html) 中 userProvider 選項的描述。

7. 儲存變更。
8. 輸出各網域的網域控制器證書，並將證書檔案複製到 Sentinel 伺服器上的 <*安裝目錄*>/config 目錄。

   如需詳細資訊，請參閱「輸出 LDAP 伺服器 CA 證書」(第 38 頁)。
9. 確定為證書檔案設定了必要的擁有權和許可。

   ```
   chown novell:novell <install_directory>/config/<cert-file>
   ```

   ```
   chmod 700 <install_directory>/config/<cert-file>
   ```
10. 將各證書新增至「設定 Sentinel 伺服器進行 LDAP 驗證」(第 39 頁) 一節之步驟 8 中建立的 KeyStore ldap_server.keystore。

    ```
    <install_directory>/jre64/bin/keytool -importcert -noprompt -trustcacerts
    -file <certificate-file> -alias <alias_name> -keystore
    ldap_server.keystore -storepass sentinel
    ```

    以 Base64 編碼格式的 LDAP 證書檔名取代 <*certificate-file*>，並以要輸入的證書別名取代 <*alias_name*>。

    重要：請確定您指定了別名。如果未指定別名，Keytool 預設會將 mykey 用作別名。將多個證書輸入至 Keystore 而未指定別名時，Keytool 會報告一個錯誤，指出該別名已經存在。

    ---
11. 啟動 Sentinel 服務。

    ```
    /etc/init.d/sentinel start
    ```

3.7.6 使用 LDAP 使用者身分證明登入

將 Sentinel 伺服器成功設定為使用 LDAP 驗證後，您可以在 Sentinel 控制中心中建立 Sentinel LDAP 使用者帳戶。如需建立 LDAP 使用者帳戶的詳細資訊，請參閱《*Sentinel Rapid Deployment User Guide*》(Sentinel Rapid Deployment 使用者指南) 中的「Creating an LDAP User Account for Sentinel」(為 Sentinel 建立 LDAP 使用者帳戶)。

建立 LDAP 使用者帳戶後，便可使用您的 LDAP 使用者名稱與密碼登入 Sentinel Rapid Deployment Web 使用者介面、Sentinel 控制中心以及 Sentinel Solution Designer。

附註：若要修改現有的 LDAP 組態，請再次執行 ldap_auth_config 程序檔，然後指定新的參數值。

3.8 將授權金鑰從試用金鑰 (Evaluation Key) 更新爲線上金鑰 (Production Key)

如果您在試用期過後購買產品，請遵循下方程序更新授權金鑰，以避免重新安裝：

1. 以 Sentinel 管理員作業系統使用者 (預設使用者爲 novell) 身分登入安裝了 Sentinel Rapid Deployment 的機器。
2. 在命令提示字元中，將目錄變更爲 < *安裝目錄* >/bin。
3. 輸入以下指令：

   ```
   ./softwarekey.sh
   ```

4. 指定 1 以設定主要金鑰。按 Enter。
5. 輸入新的有效授權金鑰，並在更新授權金鑰後遵循畫面上的指示結束。

升級 Sentinel Rapid Deployment 4

本章節提供了將 Sentinel Rapid Deployment 現有版本升級到最新修補程式的相關資訊。

附註：此修補程式只適用於 Sentinel Rapid Deployment 的 64 位元安裝版本。將此修補程式套用於 32 位元展示系統將導致安裝無法正常運作。

4.1 必要條件

- 確定要升級的系統已經安裝了 Sentinel 6.1 Rapid Deployment SP1。
- 確定 Sentinel 資料管理員工作已啓用，以便線上使用中分割區不會達到 P_MAX。如果達到 P_MAX，並且您以手動方式新增分割區，則 Sentinel 控制中心將無法成功啓動。

4.2 在伺服器上安裝修補程式

1 以 novell 使用者身分登入要安裝修補程式的伺服器。

安裝修補程式之前，請務必使用以下指令備份 Sentinel 資料庫、組態資料夾及資料資料夾：

Sentinel 資料庫：

```
tar -cf backup.tar <install_directory>/3rdparty/postgresql/
database_files
tar -cf backupdata.tar <install_directory>/3rdparty/postgresql/data
```

組態資料夾：

```
tar -cf backupconfig.tar <install_directory>/config
```

資料資料夾：

```
tar -cf backupdata.tar <install_directory>/data
```

如需這些指令的詳細資訊，請參閱 PostgreSQL 網站上的「File system level back up」(檔案系統層級備份) (http://www.postgresql.org/docs/8.1/static/backup-file.html)。

2 備份事件來源管理 (ESM) 組態並建立 ESM 輸出。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Exporting a Configuration」(輸出組態)。

3 從「Novell Patch Finder」 (Novell 修補程式搜尋工具) (http://download.novell.com/patch/finder/) 下載 Sentinel Rapid Deployment 的修補安裝程式。

4 將下載的安裝程式套件複製到暫存目錄。

5 停止 Sentinel 服務：

```
sentinel.sh stop
```

6 指定以下指令以解壓縮安裝程式套件中的檔案：

```
unzip <install_filename>
```

以安裝程式檔案的實際名稱取代 <*install_filename*>。

7 移至解壓縮後安裝程式檔案所在的目錄：

```
cd <directory_name>
```

以解壓縮後檔案所在目錄的實際名稱取代 <*directory_name*>。

8 指定以下指令以在伺服器上安裝修補程式，然後遵循畫面上的指示進行操作：

```
./service_pack.sh
```

安裝完成後，Sentinel 服務將自動啟動。

9 在執行收集器管理員和 / 或用戶端應用程式的所有機器上套用修補程式。

4.3 升級收集器管理員與用戶端應用程式

- 第 4.3.1 節「升級收集器管理員」(第 48 頁)
- 第 4.3.2 節「升級用戶端應用程式」(第 49 頁)

4.3.1 升級收集器管理員

- 「Linux」(第 48 頁)
- 「Windows」(第 48 頁)

Linux

1 以根使用者身分登入 Sentinel Rapid Deployment 收集器管理員機器。

2 從「Novell Patch Finder」(Novell 修補程式搜尋工具) (http://download.novell.com/patch/finder/) 下載 Sentinel Rapid Deployment 的修補安裝程式。

3 將下載的安裝程式檔案複製到暫存目錄。

4 指定以下指令以解壓縮安裝程式 ZIP 套件中的檔案：

```
unzip <install_filename>
```

將 <*install_filename*> 取代為安裝檔案的實際名稱。

5 移至解壓縮後安裝程式檔案所在的目錄：

```
cd <directory_name>
```

以解壓縮後安裝程式檔案所在目錄的實際名稱取代 <*directory_name*>。

6 停止收集器管理員服務。

```
<install_directory>/bin/sentinel.sh stop
```

7 執行服務套件安裝程式，然後遵循畫面上的指示進行操作：

```
./service_pack.sh
```

安裝完成後，收集器管理員服務將自動啟動。

Windows

1 以 admin 使用者身分登入 Sentinel Rapid Deployment 收集器管理員機器。

2 從「Novell Patch Finder」(Novell 修補程式搜尋工具) (http://download.novell.com/patch/finder/) 下載 Sentinel Rapid Deployment 的修補安裝程式。

3 將安裝程式檔案複製到暫存目錄。

4 解壓縮安裝程式套件中的檔案。

5 停止收集器管理員服務。

```
<install_directory>\bin\sentinel.bat stop
```

6 導覽至解壓縮後安裝程式檔案所在的目錄。

7 請執行下列操作之一以執行安裝程式：

- 連按兩下 service_pack.bat 檔案，然後遵循畫面上的指示進行操作。
- 在命令提示字元處，執行 service_pack.bat 檔案，然後遵循畫面上的指示進行操作。

安裝完成後，收集器管理員服務將自動啓動。

4.3.2 升級用戶端應用程式

Linux

1 以根使用者身分登入正在執行 Novell Sentinel Rapid Deployment 用戶端應用程式的機器。

2 從 「Novell Patch Finder」 (Novell 修補程式搜尋工具) (http://download.novell.com/patch/finder/) 下載 Sentinel Rapid Deployment 的修補安裝程式。

3 將下載的安裝程式套件複製到暫存目錄。

4 指定以下指令以解壓縮安裝程式套件中的檔案：

```
unzip <install_filename>
```

將 <*install_filename*> 取代為安裝檔案的實際名稱。

5 移至解壓縮後安裝程式檔案所在的目錄：

```
cd <directory_name>
```

以解壓縮後檔案所在目錄的實際名稱取代 <*directory_name*>。

6 執行安裝程式，然後遵循畫面上的指示進行操作：

```
./service_pack.sh
```

Windows

1 以管理員身分登入正在執行 Novell Sentinel Rapid Deployment 用戶端應用程式的機器。

2 從 「Novell Patch Finder」 (Novell 修補程式搜尋工具) (http://download.novell.com/patch/finder/) 下載 Sentinel Rapid Deployment 的修補安裝程式。

3 將下載的安裝程式檔案複製到暫存目錄。

4 解壓縮安裝程式套件中的檔案。

5 導覽至解壓縮後安裝程式檔案所在的目錄。

6 請執行下列操作之一以執行安裝程式：

- 連按兩下 service_pack.bat 檔案，然後遵循畫面上的指示進行操作。
- 在命令提示字元處，執行 service_pack.bat 檔案，然後遵循畫面上的指示進行操作。

Sentinel Rapid Deployment 的安全考量

5

本章節提供關於如何安全地安裝、設定與維護 Novell Sentinel Rapid Deployment 的特定指示。

5.1 強化

5.1.1 開箱即用強化

- 所有不必要的連接埠都已關閉。
- 在可能的情況下，服務連接埠只監聽本地連線，不允許進行遠端連線。
- 安裝檔案時只設定了最低權限，因此只有少數使用者可以讀取這些檔案。
- 不允許使用預設密碼。
- 以對資料庫只有特定許可的使用者身分執行資料庫報告。
- 所有 Web 介面都需要使用 HTTPS。
- 針對應用程式執行弱點掃描，並解決了所有潛在的安全性問題。
- 所有網路通訊預設都會使用 SSL，並針對驗證進行了相應設定。
- 使用者帳戶密碼在儲存到檔案系統或資料庫中時預設都會加密。

5.1.2 保護 Sentinel Rapid Deployment 資料的安全

因為 Sentinel Rapid Deployment 上資料的高度機密本質，您必須確保機器的實體安全，並將機器連接到安全的網路區域。若要從安全網路以外的事件來源收集資料，請使用遠端「收集器管理員」。如需遠端收集器管理員的詳細資訊，請參閱「第 3.3 節「安裝收集器管理員和用戶端應用程式」(第 30 頁)」。

5.2 保護網路之間的通訊

Sentinel Rapid Deployment 各元件會跨網路進行通訊，而且整個系統中使用了各種不同的通訊協定。

5.2.1 Sentinel 伺服器程序之間的通訊

Sentinel 伺服器程序包含 「DAS 核心」、「DAS 二進位檔案」、「關連引擎」、「收集器管理員」與 「Web 伺服器」。它們使用 ActiveMQ 與彼此通訊。

這些伺服器程序預設使用 SSL (透過 ActiveMQ 訊息匯流排) 與彼此通訊。若要設定 SSL，請在 < *安裝目錄* >/configuration.xml 中指定下列資訊：

```
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
```

如需設定自定伺服器與用戶端證書的詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Processes」(程序)。

5.2.2 Sentinel 伺服器與 Sentinel 用戶端應用程式之間的通訊

Sentinel 用戶端應用程式 (例如，Sentinel 控制中心 (SCC)、Sentinel 資料管理員 (SDM) 與 Solution Designer) 預設使用 SSL 通訊 (透過 SSL 代理伺服器)。

若要讓 Sentinel 伺服器與均以用戶端應用程式方式在伺服器上執行的 SCC、SDM 及 Solution Designer 彼此通訊，請在 < 安裝目錄 >/configuration.xml 中指定下列資訊：

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory">
   <transport type="ssl">
    <ssl host="localhost" keystore="<install_directory>/config/
.proxyClientKeystore" port="10013" usecacerts="false"/>
   </transport>
  </strategy>
```

若要讓 Sentinel 伺服器與透過網頁啓動執行的 SCC、SDM 及 Solution Designer 彼此通訊，必須以下列方式在伺服器的 < *安裝目錄* >/3rdparty/tomcat/webapps/ROOT/novellsiemdownloads/configuration.xml 檔案中定義通訊策略：

```
<strategy active="yes" id="proxied_client"
location="com.esecurity.common.communication.strategy.proxystrategy.ProxiedCl
ientStrategyFactory" >
   <transport type="ssl">
    <ssl host="127.0.0.1" port="10013" keystore="./.novell/sentinel/
.proxyClientKeystore" />
   </transport>
  </strategy>
```

如需設定自定伺服器與用戶端證書的詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Processes」(程序)。

5.2.3 伺服器與資料庫之間的通訊

伺服器與資料庫之間的通訊所使用的通訊協定是由 JDBC 驅動程式所定義。某些驅動程式可以加密與資料庫之間的通訊。

Sentinel Rapid Deployment 使用 PostgreSQL Download Page (PostgreSQL 下載頁面) (http://jdbc.postgresql.org/download.html) 提供的 PostgreSQL 驅動程式 (postgresql-< 版本 >.jdbc3.jar) 連接到 PostgreSQL 資料庫，這是一種 Java (IV 型) 實作。此驅動程式支援資料通訊加密。若要為資料通訊設定加密，請參閱 PostgreSQL Encryption Options (PostgreSQL 加密選項) (http://www.postgresql.org/docs/8.1/static/encryption-options.html)。

附註：開啓加密功能會影響系統的效能。因此，預設不會加密資料庫通訊。不過，這不會造成安全性問題，因為伺服器與資料庫之間的通訊透過迴路網路介面進行，且不會公開給開放網路。

5.2.4 收集器管理員與事件來源之間的通訊

您可以設定 Sentinel Rapid Deployment，使其以安全的方式收集來自各種事件來源的資料。不過，安全資料收集取決於事件來源所支援的特定通訊協定。例如，Check Point LEA、Syslog 以及稽核連接器設定後都可以對其與事件來源之間的通訊進行加密。

如需可啓用之安全性功能的詳細資訊，請參閱 Novell Sentinel Plug-ins Web site (Novell Sentinel 外掛程式網站) (http://support.novell.com/products/sentinel/secure/sentinelplugins.html) 上提供的連接器與事件來源廠商文件。

5.2.5 與網頁瀏覽器通訊

依預設，Web 伺服器是設定為透過 HTTPS 進行通訊。如需詳細資訊，請參閱 Tomcat documentation (Tomcat 文件) (http://tomcat.apache.org/tomcat-4.0-doc/ssl-howto.html)。

5.2.6 資料庫與其他用戶端之間的通訊

您可以設定 PostgreSQL SIEM 資料庫，以允許來自任何用戶端機器的連線，用戶端機器可以使用 Sentinel 資料管理員或任何協力廠商應用程式 (例如 Pgadmin)。

若要允許 Sentinel 資料管理員從任何用戶端機器連接，請在 < *安裝目錄* >/3rdparty/postgresql/data/pg_hba.conf 檔案加入下一行：

```
host    all         all         0.0.0.0/0               md5
```

若要限制允許執行並透過 SDM 連接到資料庫的用戶端連線，請以該主機的 IP 位址取代上一行。pg_hba.conf 中的下一行表示 PostgreSQL 會接受來自本機機器的連線，因此只允許在該伺服器上執行 Sentinel 資料管理員。

```
host all all 127.0.0.1/32 md5
```

若要限制來自其他用戶端機器的連線，您可以加入額外的 host 項目。

5.3 保護使用者與密碼

5.3.1 作業系統使用者

伺服器安裝

Sentinel Rapid Deployment 伺服器的安裝作業會建立系統使用者與群組，此使用者與群組擁有安裝在 <*安裝目錄*> 中的檔案。如果該使用者不存在，系統將建立此使用者，並將其主目錄設定為 <*安裝目錄*>。如果建立了新使用者，預設不會設定該使用者的密碼，以便確保最高安全性。如果要以安裝期間建立的使用者身分登入系統，您必須在安裝後為該使用者設定密碼。

收集器管理員安裝

系統使用者的安全性層級會有所不同，具體視安裝了收集器管理員的作業系統而定。

Linux： 安裝程式會提示您指定擁有安裝之檔案的系統使用者名稱，以及要在何處建立其主目錄。依預設，系統使用者是 esecadm；但您可以變更此系統使用者名稱。如果該使用者不存在，系統會建立此使用者與其主目錄。如果建立了新使用者，安裝期間不會設定該使用者的密碼，以便確保最高安全性。如果要以使用者身分登入系統，您必須在安裝後為該使用者設定密碼。預設群組是 esec。

安裝用戶端期間，若該使用者已存在，則安裝程式不會再提示您指定該使用者。此運作方式與解除安裝或重新安裝軟體期間的運作方式相同。不過，您可以讓安裝程式再次提示使用者：

1. 刪除第一次安裝時建立的使用者與群組
2. 從 /etc/profile 中清除環境變數 ESEC_USER

Windows：不會建立任何使用者。

系統使用者的密碼規則是由使用的作業系統定義。

5.3.2 Sentinel 應用程式與資料庫使用者

所有 Sentinel Rapid Deployment 應用程式使用者都是原生資料庫使用者，而且其密碼受原生資料庫平台所遵循的程序所保護。這些使用者只擁有資料庫中特定資料表的讀取權限，因此他們可以對資料庫執行查詢。

安裝程式會以下列使用者身分建立並設定 PostgreSQL 資料庫：

- **admin**：admin 使用者是所有 Sentinel 應用程式的管理員使用者，用於登入系統。
- **dbauser** ： dbauser 是可管理資料庫的進階使用者。dbauser 的密碼將在安裝 Sentinel Rapid Deployment 伺服器期間進行設定。此密碼儲存在 <user home directory>/.pgpass。系統會遵循 PostgreSQL 資料庫密碼規則。如需詳細資訊，請參閱第 5.3.3 節 「執行使用者的密碼規則」 (第 55 頁)。
- **appuser**：appuser 是 Sentinel 應用程式用於連接到資料庫的非進階使用者。依預設，appuser 會使用安裝期間隨機產生的密碼，該密碼儲存在 < *安裝目錄* >/config 目錄中的 XML 檔案 (das_core.xml、das_binary.xml 及 advisor_client.xml) 並於其中進行加密。若要變更 appuser 的密碼，請使用 <install_directory>/bin/dbconfig 公用程式。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment Reference Guide》*(Sentinel Rapid Deployment 參考指南) 中的「DAS Container Files」(DAS 容器檔案)。

附註：此外，還有一個 PostgreSQL 資料庫使用者擁有整個資料庫 (包含系統資料庫表格)。依預設，該 PostgreSQL 資料庫使用者設定為 NOLOGIN，因此沒有任何使用者能以 PostgreSQL 使用者身分登入。

5.3.3 執行使用者的密碼規則

Sentinel Rapid Deployment 採用基於標準的機制，讓密碼規則的執行更為容易。

安裝程式會以下列使用者身分建立並設定 PostgreSQL 資料庫：

dbauser：資料庫擁有者 (資料庫管理員使用者)。密碼是在安裝期間設定。

appuser：這是用於從 Sentinel Rapid Deployment 登入資料庫的應用程式使用者。密碼是在安裝期間隨機產生，而且僅適用於內部用途。

admin：管理員身分證明可用於登入 Sentinel Rapid Deployment Web 介面。密碼是在安裝期間設定。

依預設，使用者密碼會儲存在內嵌於 Sentinel Rapid Deployment 的 PostgreSQL 資料庫中。PostgreSQL 可以採用多種基於標準的驗證機制，如 PostgreSQL 文件的 「Client Authentication」 (用戶端驗證) (http://www.postgresql.org/docs/8.3/static/client-authentication.html) 一章中所述。

採用這些機制會影響 Sentinel Rapid Deployment 中的所有使用者帳戶，包括 Web 應用程式的使用者以及僅用於後端服務的帳戶，例如 dbauser 與 appuser。

一個更為簡單的選項是使用 LDAP 目錄驗證 Web 應用程式使用者。若要在 Sentinel Rapid Deployment 伺服器上啟用此選項，請參閱第 3.7 節 「LDAP 驗證」 (第 37 頁)。此選項對後端服務所使用的帳戶不會產生任何影響，除非您變更 PostgreSQL 組態設定，否則這些帳戶將繼續透過 PostgreSQL 進行驗證。

您可以使用這些基於標準的機制和您環境 (如 LDAP 目錄) 中的現有機制，來實現穩固的 Sentinel Rapid Deployment 密碼規則執行。

5.4 保護 Sentinel 資料

重要：因為 Sentinel 伺服器上之資料的高度機密本質，您應該確保機器的實體安全，並將機器連接到安全的網路區域。若要從安全網路以外的事件來源收集資料，請使用遠端「收集器管理員」。

對於特定元件，您必須儲存密碼，以便在系統需要連接到特定資源 (例如，例如資料庫或事件來源) 時使用。在此案例中，當您儲存密碼時，會先將密碼加密以避免未經授權的使用者存取明文密碼。

即使密碼已經過加密，您仍必須小心地設定對於所儲存密碼資料的存取權，以避免密碼曝光。例如，您可以確定未經授權的使用者無法讀取包含機密資料之檔案上的權限。

檔案

advisor_client.xml

資料庫身分證明

資料庫身分證明儲存在 < *安裝目錄* >/config/server.xml 檔案中

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

Advisor 身分證明

```
<obj-component id="DownloadComponent">
          <class>esecurity.ccs.comp.advisor.feed.NewAdvClientDownload</class>
      <property name="advisor.downloadfrom.url">https://secure-www.novell.com/
sentinel/advisor/advisordata</property>
      <property name="username">admin</property>
      <!-- Set the password (encrypted) using the adv_change_password script -
->
      <property name="password">jqhlWIX8HD6GDHVX9FApWg==</property>
<property name="compression.enabled">true</property>
      <!--
        Set the following properties to connect through an HTTP proxy.
       Set the proxy password (encrypted) using the adv_change_password script
(make a
        copy of the script and add "-x" to the java cmd line to set the proxy
password
        instead of the advisor password.
      -->
      <!--
      <property name="proxy_host"></property>
      <property name="proxy_port"></property>
      <property name="proxy_username"></property>
      <property name="proxy_password"></property>
      -->
        </obj-component>
```

Configuration.xml

```
<strategy active="yes" id="jms"
location="com.esecurity.common.communication.strategy.jmsstrategy.activemq.Ac
tiveMQStrategyFactory" name="ActiveMQ">
<jms brokerURL="failover://(ssl://
localhost:61616?wireFormat.maxInactivityDuration=30000)?randomize=false"
interceptors="compression" keystore="../config/.activemqclientkeystore.jks"
keystorePassword="password" password="374d9f338b4dc4b50e45b3822fc6be12"
username="system"/>
    </strategy>
```

das_binary.xml

```
<class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

das_core.xml

```
 <class>esecurity.base.ccs.comp.dataobject.ConnectionManager</class>
    <property name="username">appuser</property>
    <property name="password">7fA+ogBMeK7cRbJ+S6xJ/
InLBUi+sRVGK5qYycDxfIqGDHVX9FApWg==</property>
```

部分資料庫表格會儲存密碼與證書。此機密資料已加密，並會儲存在下面列出的表格中。您必須限制對於這些資料表的存取權。

- **evt_src_**：evt_src_config 欄位資料
- **evt_src_collector**：欄位：evt_src_collector_props
- **evt_src_grp (doubt)**：欄位：evt_src_default_config
- **md_config** ： 欄位：data
- **integrator_config** ： 欄位：integrator_properties
- **md_view_config** ： 欄位：view_data
- **esec_content** ： 欄位：content_context、content_hash
- **esec_content_grp_content** ： 欄位：content_hash
- **sentinel_plugin**：欄位：content_pkg、file_hash

Sentinel Rapid Deployment 會儲存組態資料與事件資料。此資料儲存在下列位置：

元件	組態資料的位置	事件資料的位置
Sentinel Rapid Deployment 伺服器	資料庫表格與檔案系統 (< *安裝目錄* >/config) 此組態資訊包含加密的資料庫、事件來源、整合器與密碼。	資料庫 (EVENTS、CORRELATED_EVENTS、EVT_SMRY_ 及 AUDIT_RECORD 表格) 與檔案系統的以下位置： < *安裝目錄* >/data/eventdata 與 < *安裝目錄* >/data/raw data 事件資料可在分割區管理工作中歸檔到檔案系統。

元件	組態資料的位置	事件資料的位置
關連引擎	檔案系統 (< *安裝目錄* >/config)。唯一的機密組態資訊是用於連接到訊息匯流排的用戶端金鑰組。	correlation_engine.cache
DAS 核心	< *安裝目錄* >/config	das_core.cache
DAS 二進位檔案	< *安裝目錄* >/config	若資料庫已關閉，系統可能會快取事件資料。 das_binary.cache
收集器管理員	檔案系統 (< *安裝目錄* >/config)。唯一的機密組態資訊是用於連接至訊息匯流排的收集器管理員使用者密碼。	發生錯誤時 (例如訊息匯流排 已關閉或事件溢位)，系統可能會將事件資料快取在檔案系統上。此事件資料儲存在 < *安裝目錄* >/data/collector_mgr.cache 目錄中。
用戶端應用程式	檔案系統 (*安裝目錄* /config)。用戶端應用程式不會在其組態檔案中儲存任何機密資訊。 例如，用戶端應用程式可以將 ESM 資料輸出到本機檔案系統。輸出的檔案包含加密的密碼 (如果它們存在於輸出的事件來源組態中)。雖然密碼已加密，您應該只將 ESM 輸出權限授予信任的使用者。	無

5.5 備份資訊

- 必須定期備份事件。備份媒體應該存放在安全的異地設備中。
- 備份系統資料。如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「Backup and Restore Utility」(備份與還原公用程式)。
- 對於機密資料，請使用下列其中一種方式將資料備份加密：
    - 加密資料本身 (若建立資料的應用程式支援加密)。例如，資料庫產品與協力廠商工具支援資料加密。使用可在備份資料時加密資料的備份軟體。這種方式對於效能與管理性是一種挑戰，特別是在管理加密金鑰方面。
    - 使用可在備份資料時加密機密備份媒體的加密裝置。
- 若要將媒體傳送並儲存在異地，請委託專門運送及儲存媒體的公司處理。確定您的磁帶已加上追蹤條碼、儲存在適當的環境中，而且委由專門處理媒體、聲譽良好的公司處理。
- 載入復原證書。預設不會針對復原代辦設定 Novell Sentinel 服務。透過 YaST 設定伺服器組態期間，請確定已設定復原代辦路徑。此路徑應該包含可供服務載入的證書清單，以便使用者選取證書。

  如需詳細資訊，請參閱 《*Sentinel Rapid Deployment Reference Guide*》 (Sentinel Rapid Deployment 參考指南) 中的 「Certificate Management for Sentinel 6.1 Rapid Deployment Server」(Sentinel 6.1 Rapid Deployment 伺服器的證書管理)。

  YaST 包含用於 X.509 證書的基本管理模組，主要與建立 CA、子 CA 以及其證書有關。如需有關如何管理及更新證書的詳細資訊，請參閱 *《SUSE Linux Enterprise Server 10 Installation and Administration Guide (SUSE Linux Enterprise Server 10 安裝與管理指南)*

(http://www.novell.com/documentation/sles10/sles_admin/data/bookinfo_book_sles_admin.html) 中的 Managing X.509 Certification (管理 X.509 證書) (http://www.novell.com/documentation/sles10/sles_admin/data/cha_yast_ca.html)。

5.6 保護作業系統

- SUSE Linux Enterprise Server (SLES) 10 SP3 或更新版本支援 Sentinel Rapid Deployment。如需保護 SLES 機器安全的詳細資訊，請參閱 SUSE Linux Enterprise Server 10 documentation (SUSE Linux Enterprise Server 10 文件) (http://www.novell.com/documentation/sles10/sles_admin/data/part_security.html)。
- 使用防火牆保護對於 Sentinel Rapid Deployment 伺服器的存取。若要允許從公司網路外部存取 Sentinel 伺服器，您應該使用防火牆，避免入侵者存取 Sentinel 伺服器。

  在防火牆開啓下列連接埠：

元件	連接埠
ActiveMQ	61616
PostgreSQL	5432
Tomcat	8443
Sentinel 控制中心代理用戶端連接埠	10013
代理信任的用戶端	10014
引擎與管理員之間使用的 internal_gateway_server 與 internal_gateway	5556
internal_router_server 與 internal_router_client 在事件路由器用戶端與伺服器之間使用	5558
事件監聽埠 於 config/collector_mgr.properties 中透過 「esecurity.agentmanager.event.port」進行設定	35000

附註：如果安裝時以星號標示的連接埠已在使用中，則這些連接埠可能會不同。安裝時若那些連接埠已被使用，請以安裝時提示的連接埠號碼來取代這些連接埠。

如需在 SLES 10 啓動防火牆的詳細資訊，請參閱 《*SLES 10 Administration Guide*》 (SLES 10 管理指南) 中的 Configuring Firewalls with YaST (使用 YaST 來設定防火牆) (http://www.novell.com/documentation/sles10/sles_admin/data/sec_fire_suse.html)。

5.7 檢視 Sentinel 稽核事件

Sentinel Rapid Deployment 會針對使用者執行的多種動作及系統活動內部執行的動作產生稽核事件。您可以在 Active View 檢視這些事件，或透過搜尋或報告功能來存取這些事件。不過，您必須擁有必要的許可才能檢視系統事件。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment User Guide*》 (Sentinel Rapid Deployment 使用者指南) 中的 「System Events for Sentinel」(Sentinel 的系統事件)。

5.8 使用 CA 證書

您可以使用由主要證書管理中心 (CA) (例如 VeriSign、Thawte 或 Entrust) 所簽署的證書來取代自行簽署的證書。您也可以使用由較不常用的 CA (例如您公司或組織中的 CA) 所簽署的證書來取代自行簽署的證書。

如需詳細資訊，請參閱 《*Sentinel Rapid Deployment Reference Guide*》 (Sentinel Rapid Deployment 參考指南) 中的 「Certificate Management for Sentinel 6.1 Rapid Deployment Server」(Sentinel 6.1 Rapid Deployment 伺服器的證書管理)。

測試 Sentinel Rapid Deployment 的功能 6

Sentine Rapid Deployment 會連同一般收集器一起安裝，可用於測試系統的許多基本功能。您可以使用此收集器測試主動檢視、事件建立、關連規則以及報告。

6.1 測試 Rapid Deployment 安裝

下列程序說明測試 Sentinel Rapid Deployment 系統的步驟及預期結果。您可能不會看到相同的事件，不過結果應該會與下方的結果類似。

基本上，這些測試可讓您確認下列事項：

- Sentinel 服務已啓動且正在執行。
- 訊息匯流排的通訊正在進行。
- 內部稽核事件正在傳送。
- 可從收集者管理員傳送事件。
- 事件會被插入資料庫，而且您可以使用報告來取回事件。
- 可建立並檢視事件。
- 關連引擎會評估規則並觸發關連的事件。
- Sentinel 資料管理員會連接到資料庫，並且可以讀取分割區資訊。

如果任何測試失敗，請檢視安裝記錄和其他記錄檔，若有需要請與 「Novell 技術支援 (NTS)」(http://support.novell.com/phone.html?sourceidint=suplnav4_phonesup) 聯絡。

若要測試應用程式，請執行下列動作：

1 登入 Sentinel Rapid Deployment Web 介面。

如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Accessing the Novell Sentinel Web Interface」(存取 Novell Sentinel Web 介面)。

2 選取 「搜尋」頁面，然後搜尋任何內部事件。應該會傳回一或多個事件。

例如，若要在嚴重性範圍 3-5 內搜尋內部事件，請選取 *「包含系統事件」*，然後在 *「搜尋」*欄位中輸入 *sev:[3 TO 5]*。

如需搜尋的詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Running an Event Search」(執行事件搜尋)。

在 SP2 中，預設不會啓用 「搜尋」功能。但是，如果要啓用此功能，請參閱 *《Sentinel Rapid Deployment User Guide》*(Sentinel Rapid Deployment 使用者指南) 中的 「Enabling the Search Option in Web User Interface」(啓用 Web 使用者介面中的搜尋選項)。

3 選取 「報告」頁面並指定參數，然後執行報告。

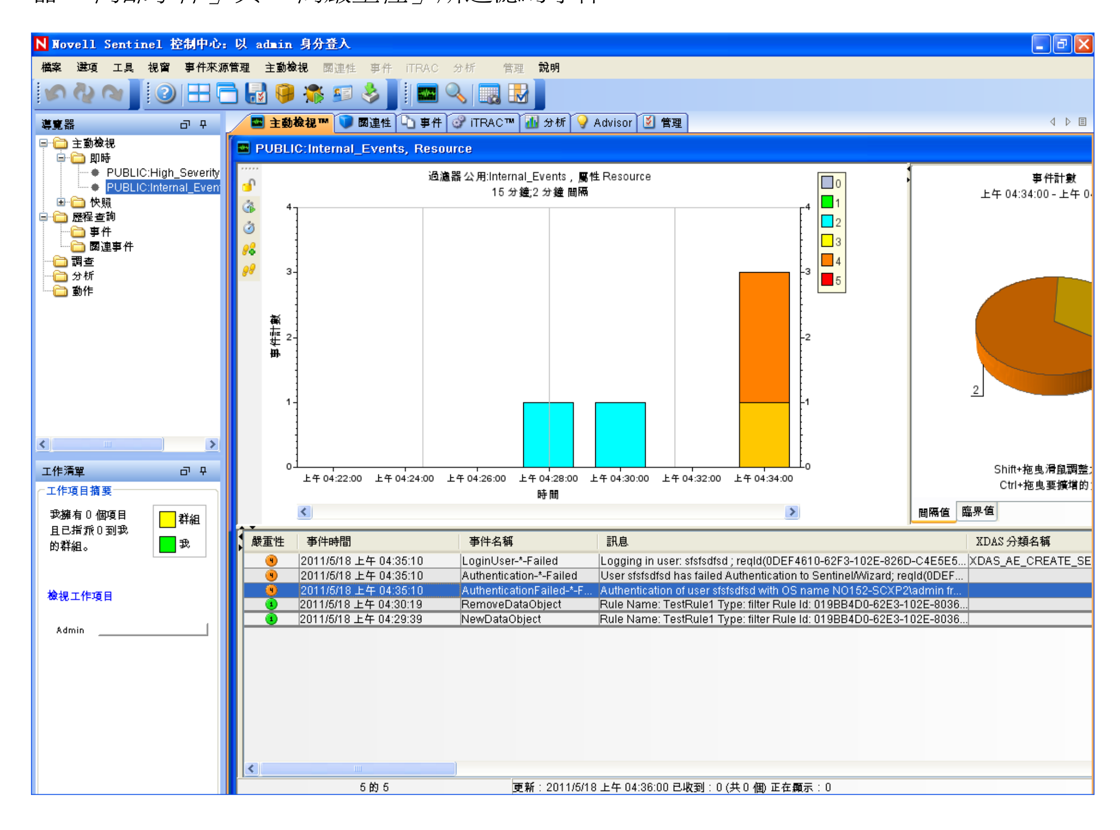
例如，按一下 Sentinel 核心事件組態旁的 *「執行」*按鈕，指定所需參數，然後按一下 *「執行」*。

如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》* (Sentinel Rapid Deployment 使用者指南) 中的 「Running Reports」(執行報告)。

4 在 「應用程式」頁面中，按一下 *「啟動 Sentinel 控制中心」*。

5 使用安裝期間所指定的 Sentinel 管理使用者登入系統 (預設為 admin)。

Sentinel 控制中心隨即開啟並顯示 *「主動檢視」*索引標籤，此索引標籤顯示以公用過濾器 *「內部事件」*與 *「高嚴重性」*所過濾的事件。



6 移至 *「事件來源管理」*功能表，然後選取 *「即時檢視」*。

7 在圖形檢視中，在 *「5 eps 事件來源」*上按一下滑鼠右鍵，然後選取 *「啟動」*。

8 關閉 「事件來源管理即時檢視」視窗。

9 按一下 *「Active View」*索引標籤。

您可以檢視標題為 「公用：高嚴重性、嚴重性」的使用中視窗。啟動收集器以及在此視窗中顯示資料可能需要一些時間。

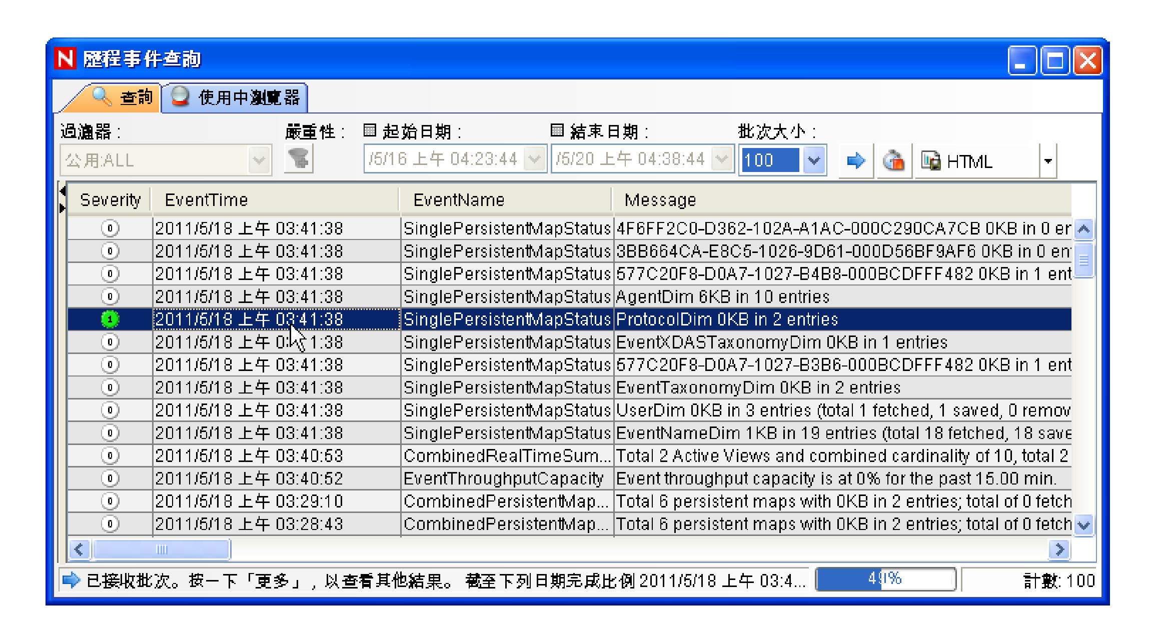
10 按一下工具列上的 *「事件查詢」*按鈕。「歷程事件查詢」視窗即會顯示。

11 在 「歷程事件查詢」視窗中，按一下 *「過濾器」*向下箭頭以選取過濾器。選取 *「公用 : 全部」*過濾器。

12 選取收集器運作時間的時段。使用 *「自」*與 *「至」*下拉式清單選取日期範圍。

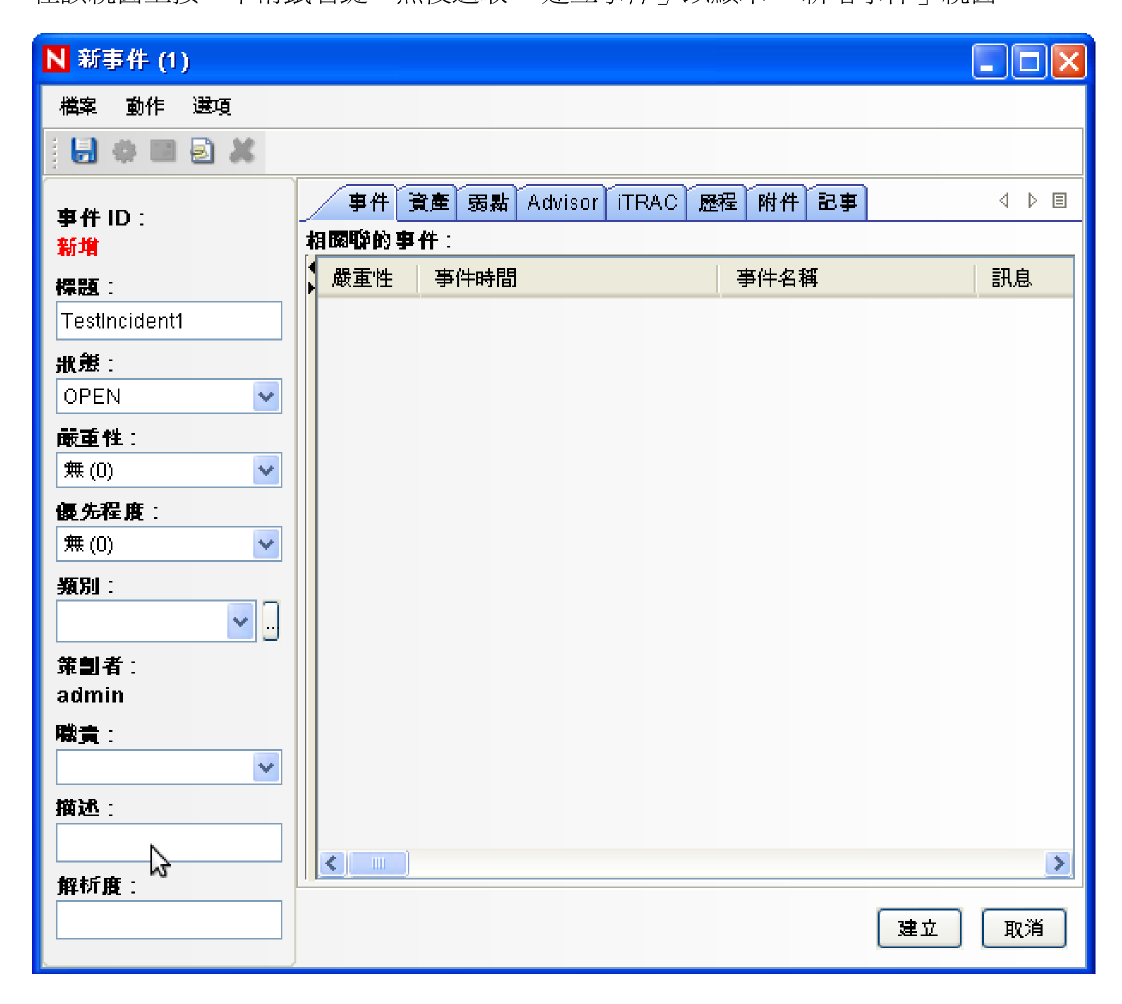
13 選取批次大小。

14 按一下放大鏡圖示以執行查詢。



15 按住 Ctrl 鍵或 Shift 鍵，然後從「歷程事件查詢」視窗中選取多個事件。

16 在該視窗上按一下滑鼠右鍵，然後選取*「建立事件」*以顯示「新增事件」視窗。

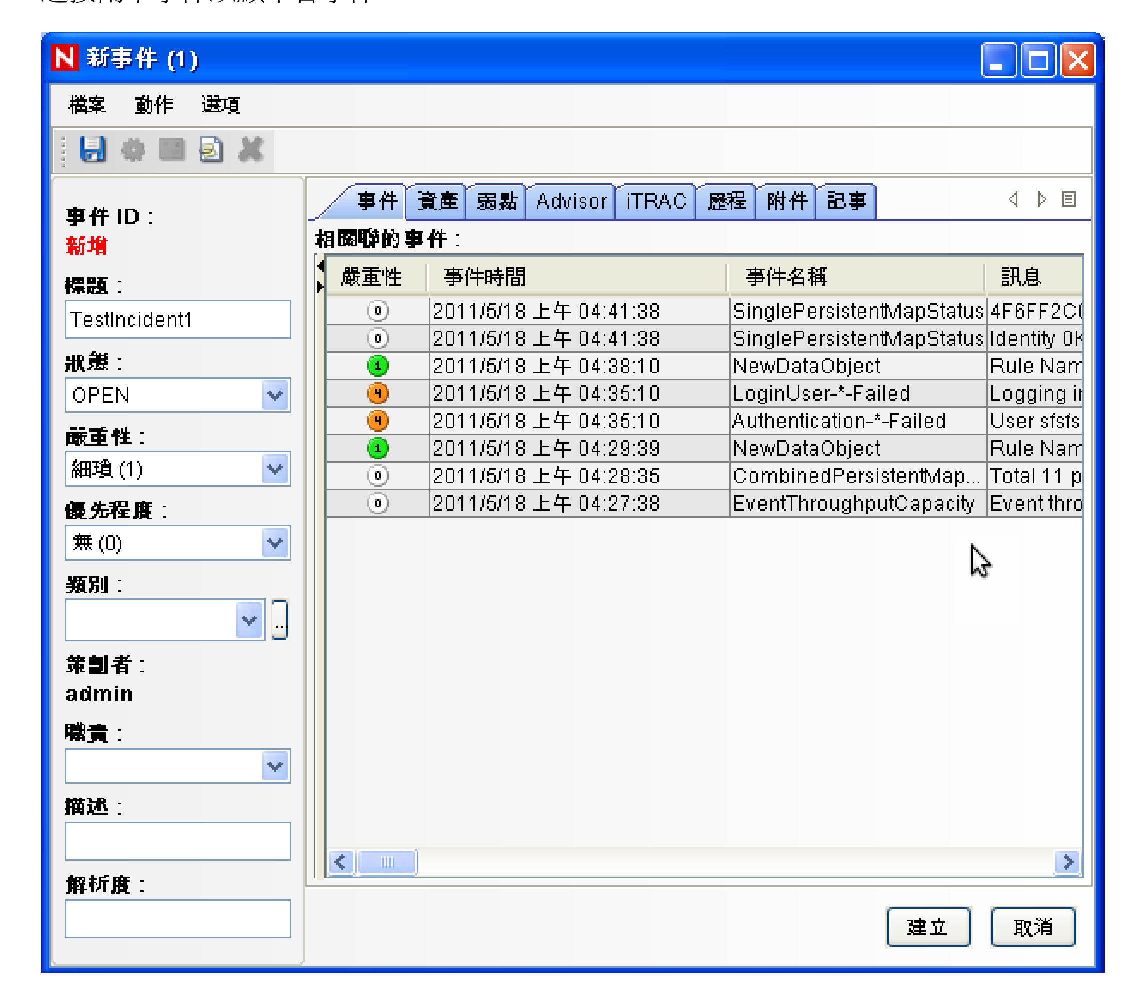


17 將事件命名為 TestIncident1，然後按一下 *「建立」*。顯示成功通知後，按一下 *「儲存」*。

18 按一下 *「事件」*索引標籤檢視剛才在「事件檢視窗管理員」中建立的事件。



19 連按兩下事件以顯示各事件。



20 關閉「事件」視窗。

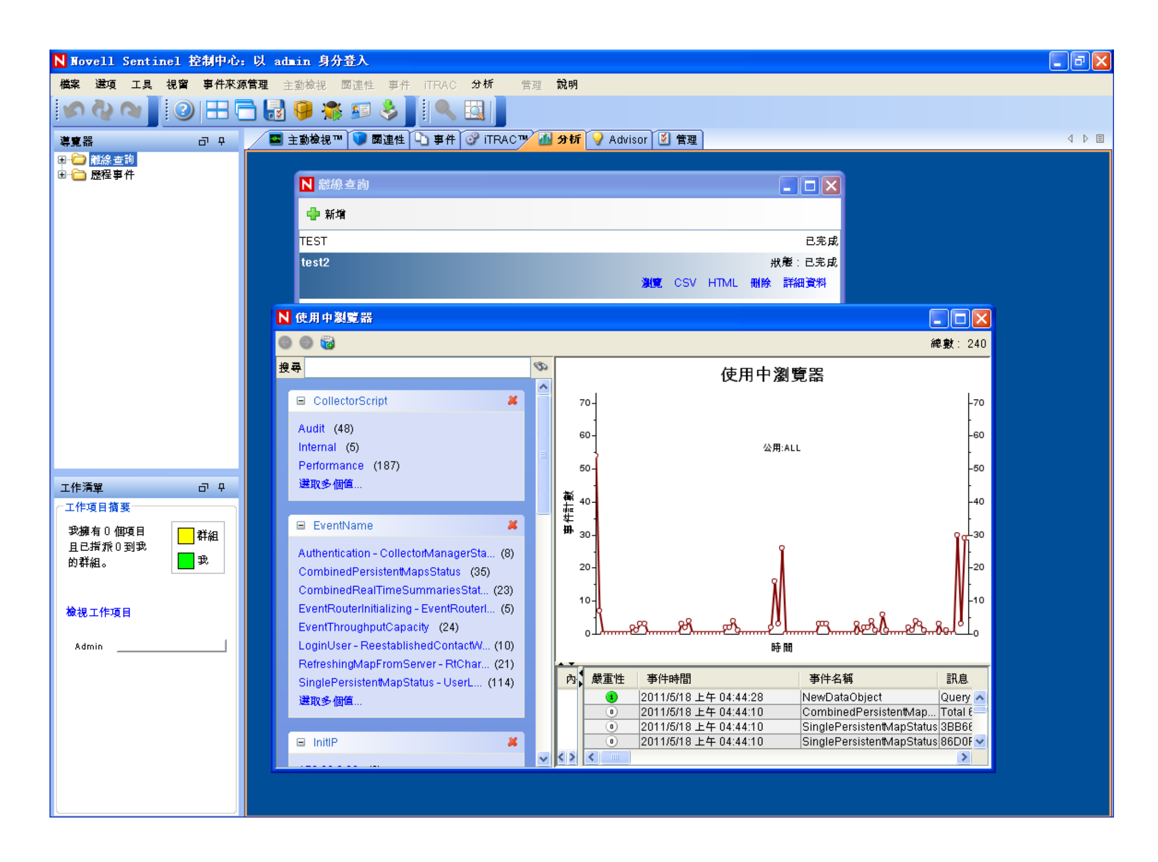
21 按一下 *「分析」*索引標籤。

22 按一下 *「分析」*功能表或導覽器中的 *「離線查詢」*。

23 在「離線查詢」視窗中，按一下 *「新增」*。

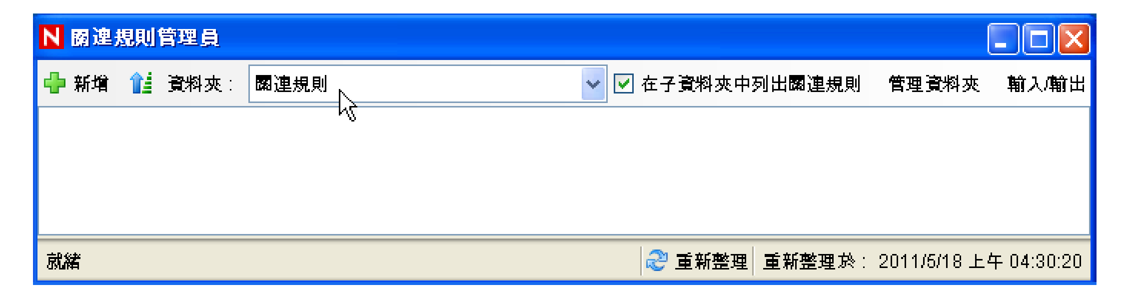
24 指定名稱，依次選取過濾器與時段，然後按一下 *「確定」*。

25 按一下 *「瀏覽」*以檢視「使用中瀏覽器」視窗中的事件清單和相關詳細資料。



您可以檢視收集器、目標 IP、嚴重性、目標服務連接埠以及資源等詳細資料。

26 選取 *「關連」*索引標籤。「關連規則管理員」即會顯示。



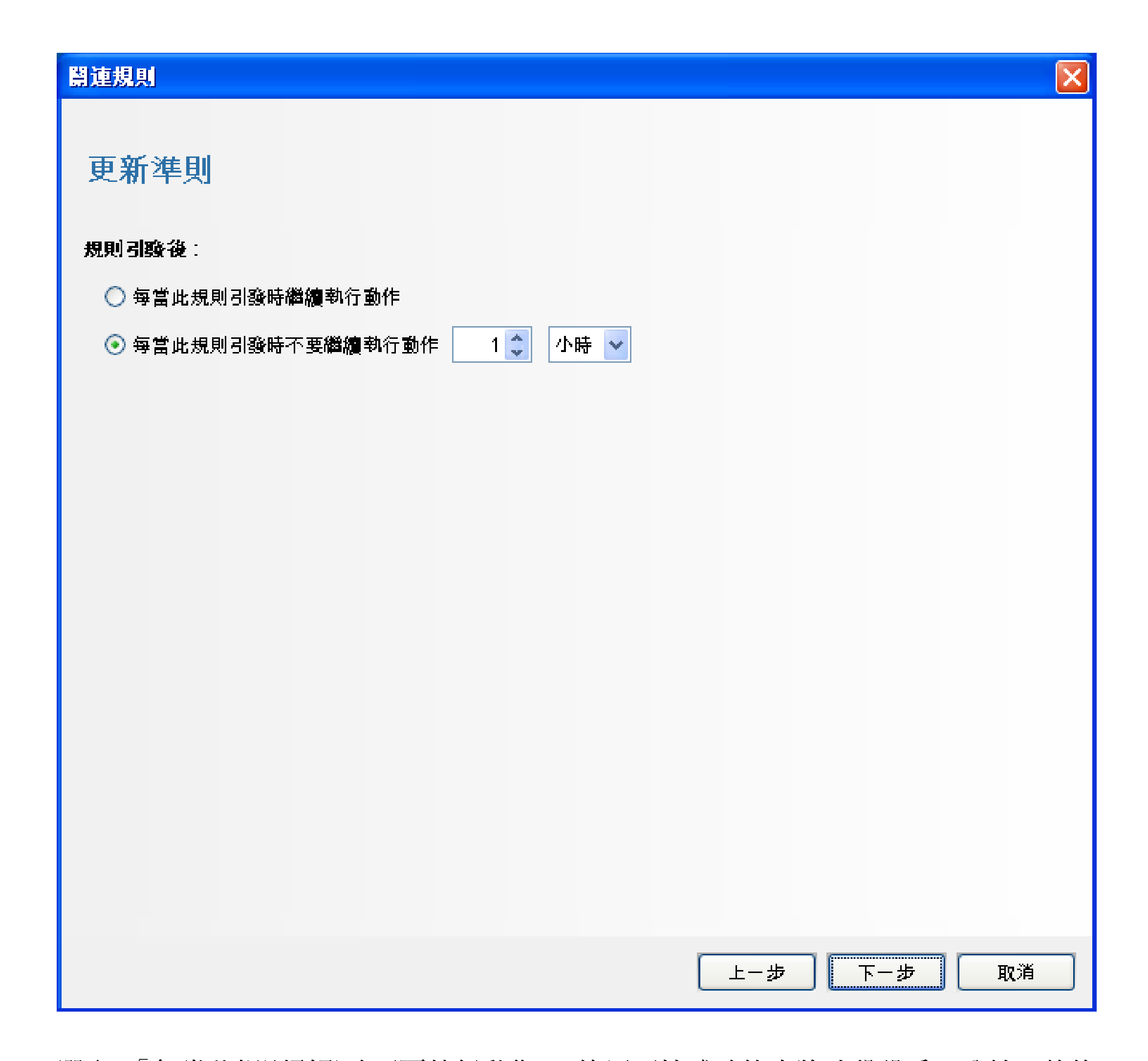
27 按一下 *「增加」*。「關連規則精靈」即會顯示。



28 按一下 *「簡易」*。「簡易規則」視窗即會顯示。



29 使用下拉式功能表將準則設為「嚴重性 = 4」，然後按「*下一步*」。「更新準則」視窗即會顯示。



30 選取 「*每當此規則引發時不要執行動作*」，使用下拉式功能表將時段設為 1 分鐘，然後按 「*下一步*」。「一般描述」視窗即會顯示。



31 將規則命名為 *TestRule1*，輸入描述，然後按 *「下一步」*。

32 選取 *「否，不要建立其他規則」*，然後按 *「下一步」*。

33 建立與所建立之規則關聯的動作：

33a 執行以下任一操作：

- 選取 *「工具」* > *「動作管理員」* > *「新增」*。
- 在 「部署規則」視窗中，按一下 *「新增動作」*。如需詳細資訊，請參閱步驟 35 (第 70 頁)至步驟 34。

「設定動作」視窗即會顯示。



33b 在「設定動作」視窗中，指定以下項目：

- 指定動作名稱，例如「關連事件動作」。
- 從*「動作」*下拉式清單中選取*「設定關連事件」*。
- 設定*「事件選項」*。
- 將*「嚴重性」*設為 5。
- 指定*「事件名稱」*，例如「關連事件」。
- 根據需要指定訊息。

如需建立動作的詳細資訊，請參閱*《Sentinel Rapid Deployment User Guide》*(Sentinel Rapid Deployment 使用者指南) 中的「Creating Actions」(建立動作)。

33c 按一下*「儲存」*。

34 開啓「關聯性規則管理員」視窗。

35 選取規則，然後按一下*「部署規則」*連結。「部署規則」視窗即會顯示。

36 在「部署規則」視窗中，選取用於部署規則的引擎。

37 選取步驟 33 (第 69 頁) 中建立的動作以與該規則關聯，然後按一下*「確定」*。



38 選取 *「關連引擎管理員」*。

您會在關連引擎下方看到規則已部署並啓用。



39 觸發嚴重性爲 4 的事件 (例如驗證失敗) 以引發部署的關連規則。

例如，開啓 Sentinel 控制中心登入視窗，然後指定錯誤的使用者身分證明以產生此類事件。

40 按一下 *「主動檢視」*索引標籤，然後驗證關連事件是否已產生。

嚴重性	事件時間	事件名稱	訊息	XDAS 分類名稱
1	2011/5/18 上午 04:18:51	NewDataObject	Action Name: CorrelatedEvent with Id: 019BB4D0-62E3-102E-8004-00...	
1	2011/5/18 上午 04:16:53	UpdateDataObject	Updating Config Object: Preferences by User: admin; reqId(75CEF260-...	
1	2011/5/18 上午 04:16:49	RtChartJoiningExistingD...	Joined existing Active View with filter _SYSTEM:Internal_Events and attr...	
1	2011/5/18 上午 04:16:49	RtChartJoiningExistingD...	Joined existing Active View with filter _SYSTEM:High_Severity and attri...	
1	2011/5/18 上午 04:16:47	LoginUser	Logging in user: admin ; reqId(75CEF260-62F0-102E-AD24-462530D7...	XDAS_AE_CREATE_SE

41 關閉 Sentinel 控制中心。

42 在「應用程式」頁面中，按一下 *「啓動 Sentinel 資料管理員」*。

43 使用安裝期間指定的資料庫管理使用者登入 Sentinel 資料管理員 (預設爲 dbauser)。



44 按一下每個索引標籤，驗證是否可以存取。

45 關閉「Sentinel 資料管理員」。

如果您已完成所有步驟且沒有發生任何錯誤，則表示您已完成 Sentinel 系統安裝的基本驗證工作。

6.2 測試後的清理

完成系統驗證後，您應該移除測試作業所建立物件。

1 使用安裝期間所指定的 Sentinel 管理使用者登入系統 (預設爲 admin)。

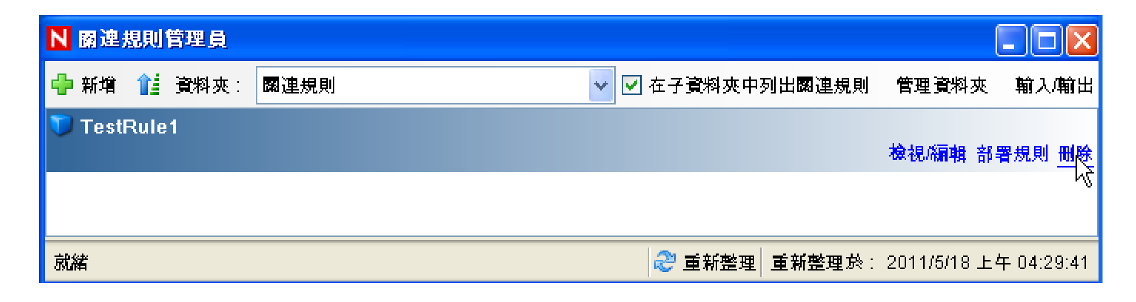
2 選取 *「關連」*索引標籤。

3 開啓「關聯性引擎管理員」。

4 在關連引擎管理員中的 *TestRule1* 上按一下滑鼠右鍵，然後選取 *「解除部署」*。

5 開啓「關聯性規則管理員」。

6 選取 *TestRule1*，然後按一下 *「刪除」*。



7 選取 *「工具」* > *「動作管理員」*以顯示「動作管理員」視窗。

8 選取 *「關連事件」*動作，按一下 *「刪除」*，然後按一下 *「是」*確認刪除操作。



9 選取 *「事件來源管理」*功能表，然後選取 *「即時檢視」*。

10 在「圖形」事件來源階層中，在 *「一般收集器」*上按一下滑鼠右鍵，然後選取 *「停止」*。

11 關閉「事件來源管理」視窗。

12 按一下 *「事件」*索引標籤。

13 開啓「事件檢視管理員」。

14 選取 *「TestIncident1」*並按一下滑鼠右鍵，然後選取 *「刪除」*。

6.3 使用實際資料

若要開始處理實際資料，您必須輸入並設定其適合環境的收集器，設定您自己的規則，並建立 iTRAC 工作流程等。如需詳細資訊，請參閱 *《Sentinel Rapid Deployment User Guide》*(Sentinel Rapid Deployment 使用者指南)。「Sentinel 解決方案套件」可協助您快速上手。如需詳細資料，請參閱 Sentinel Content Page (Sentinel 內容網頁) (http://support.novell.com/products/sentinel/sentinel61.html)。

解除安裝 Sentinel Rapid Deployment

7

7.1 解除安裝 Sentinel Rapid Deployment 伺服器

1 以 root 使用者的身分登入。

2 移至 setup 目錄。

```
cd <install_directory>/setup
```

3 執行 uninstall.sh 程序檔以解除安裝 Sentinel Rapid Deployment 伺服器：

```
./uninstall.sh
```

程序檔會以訊息方式提示您，該訊息指出 Sentinel Rapid Deployment 將完全移除。

4 指定在解除安裝 Sentinel Rapid Deployment 伺服器時是要保留還是移除使用者。按 y 移除使用者，按 n 保留使用者。

5 指定在解除安裝 Sentinel Rapid Deployment 伺服器時是要保留還是移除群組。按 y 移除群組，按 n 保留群組。

6 按 y 解除安裝，按 n 結束解除安裝。

7.2 解除安裝 「遠端收集器管理員」與 Sentinel 用戶端應用程式

7.2.1 Linux

1 以 root 的身分登入。

2 (視情況而定) 如果您要解除安裝收集器管理員，請停止 Sentinel Rapid Deployment 服務：

```
<install_directory>/bin/sentinel.sh stop
```

3 移至下列位置：

```
<install_directory>/_uninst
```

4 執行以下任一操作：

模式	指令
GUI	`./uninstall.bin`
	請繼續執行步驟 5 (第 76 頁)。
主控台	`./uninstall.bin -console`
	依照畫面上顯示的指示執行。

5 選取語言，然後按一下 *「確定」*。
6 在 Sentinel UninstallShield 精靈中，按一下 *「下一步」*。
7 選取您要解除安裝的元件，然後按一下 *「下一步」*。
8 確定所有執行中的 Sentinel 應用程式都已停止，然後按一下 *「下一步」*。
隨即顯示已選取要解除安裝的功能摘要。
9 按一下 *「解除安裝」*。
10 按一下 *「完成」*。

7.2.2 Windows

1 以 「管理員」使用者身分登入。
2 (視情況而定) 如果您要解除安裝收集器管理員，請停止 Sentinel Rapid Deployment 服務：
`<install_directory>\bin\sentinel.bat stop`
3 執行下列一項動作：
   - 選取 *「開始」* > *「所有程式」* > *「Sentinel」* > *「解除安裝 Sentinel」*。
   - 選取 *「開始」* > *「執行」*，輸入 < *安裝目錄* >_uninst，然後連按兩下 uninstall.exe。
4 選取語言，然後按一下 *「確定」*。
隨即顯示 Sentinel Rapid Deployment UninstallShield 精靈。
5 按一下 *「下一步」*。
6 選取您要解除安裝的元件，然後按一下 *「下一步」*。
7 確定所有執行中的 Sentinel 應用程式都已停止，然後按一下 *「下一步」*。
隨即顯示已選取要解除安裝的功能摘要。
8 按一下 *「解除安裝」*。
9 選取重新啓動系統的選項，然後按一下 *「完成」*。

7.2.3 解除安裝後的程序

解除安裝應用程式之後會留下特定系統設定，您可以手動移除這些設定。請先移除這些設定，再執行 Sentinel 全新安裝，尤其是 Sentinel 解除安裝期間發生錯誤時更是如此。

附註：在 Linux 上，解除安裝 「收集器管理員」或用戶端應用程式並不會從作業系統移除「Sentinel 管理員使用者」。若需要，您必須手動移除該使用者。

- 「Linux」 (第 77 頁)
- 「Windows」 (第 77 頁)

Linux

1 以 root 的身分登入。

2 移除 <*安裝目錄*> (Sentinel 軟體安裝位置) 的內容。

3 移除 /etc/init.d 目錄中的下列檔案 (如果存在)：

   sentinel

   僅適用於已安裝 「收集器管理員」的情況。

4 確定沒有任何使用者以 「Sentinel 管理員」使用者 (預設是 esecadm) 的身分登入，然後移除該使用者、主目錄與 esec 群組：
   - 執行 userdel -r esecadm
   - 執行 groupdel esec

5 移除 /root/InstallShield 目錄。

6 移除 /etc/profile 中的 InstallShield 區段。

7 重新啓動機器。

Windows

1 刪除 %CommonProgramFiles%\InstallShield\Universal 資料夾與該資料夾下的所有內容。

2 刪除 <*安裝目錄*> 資料夾 (預設值為：C:\Program Files\Novell\Sentinel6)。

3 用滑鼠右鍵按一下 *「我的電腦」* > *「內容」* > *「進階」*索引標籤。

4 按一下 *「環境變數」*按鈕。

5 如果有下列變數，請予以刪除：
   - ESEC_HOME
   - ESEC_VERSION
   - ESEC_JAVA_HOME
   - ESEC_CONF_FILE
   - WORKBENCH_HOME

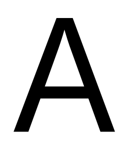
6 移除指向 Sentinel 安裝的 Path 環境變數中的任何項目。

7 刪除桌面上的所有 Sentinel 捷徑。

8 從 *「開始」*功能表刪除 *「開始」* > *「程式集」* > *「Sentinel」*捷徑資料夾。

9 重新啓動機器。

更新 Sentinel Rapid Deployment 主機名稱



A.1 伺服器

在 Sentinel 伺服器上，執行期間或安裝期間會自動更新主機名稱變更。若更新主機名稱後伺服器無法正常運作，您必須手動檢查下列項目：

- 重新啟動 Sentinel 後，所有 jnlp 檔案與 configuration.xml 檔案都已更新。
- sentinel_host 資料庫資料表中的主機名稱項目已更新。
- < *安裝目錄* >/config/configuration.xml 檔案中對於本機迴路 (localhost 或 127.0.0.1) 的所有參照都未受影響。

A.2 用戶端應用程式

對於用戶端應用程式，您必須手動變更下列位置中的伺服器主機名稱或 IP 位址，以指向正確的伺服器：

- < *安裝目錄* >/config/configuration.xml。

  「Sentinel 控制中心」與 Solution Designer 使用此資訊。
- < *安裝目錄* >/config/SentinelPreferences.properties 檔案中提供的說明 URL。
- 執行下列指令以更新 sdm.connect 檔案中的主機名稱：

```
sdm -action saveConnection -server <postgresql> -host <hostIpaddress/
hostName> -port <portnum> -database <databaseName/SID> [-driverProps
<propertiesFile] {-user <dbUser> -password <dbPass> | -winAuth} -
connectFile <filenameToSaveConnection>
```

疑難排解秘訣

B

本節提供疑難排解建議清單，可協助您解決一些 Sentinel Rapid Deployment 安裝問題。

B.1 輸入無效的身分證明而導致資料庫驗證失敗

常見原因：如果在將 Sentinel Rapid Deployment 伺服器設定爲使用 LDAP 驗證的過程中輸入了無效的 LDAP 伺服器主機名稱或 IP 位址，則資料庫驗證將會失敗。

動作：請確定輸入的 LDAP 伺服器主機名稱或 IP 位址有效。

B.2 Sentinel Web 介面無法啓動

常見原因：您在正在執行 Identity Audit 程序的機器上安裝 Sentinel Rapid Deployment，或其解除安裝程序未完成。

動作：Sentinel Rapid Deployment 與 Novell Identity Audit 不能安裝在同一台機器上。在安裝了 Identity Audit 的機器上安裝 Sentinel Rapid Deployment 之前，請確保您已完全解除安裝 Identity Audit。

如果 Identity Audit 程序未完全停止，將無法成功完成 Identity Audit 的解除安裝程序。在這種情況下，安裝 Sentinel Rapid Deployment 或啓動其應用程式時可能會發生衝突。

1. 執行下列指令以關閉 Identity Audit 服務：

   ```
   /etc/init.d/identity_audit stop
   ```

2. 執行下列指令以確保所有 Identity Audit 都已停止運作：

   ```
   ps -ef | grep novell
   ```

3. 如果有需要，請手動停止所有剩餘的程序。

   ```
   kill -9 pid
   ```

4. 使用必要的根許可解除安裝 Identity Audit。

   如需詳細資訊，請參閱 《Identity Audit Guide》 (Identity Audit 指南) (http://www.novell.com/documentation/identityaudit/identityaudit10guide/data/)。

B.3 啓用 UAC 時，Windows 2008 上的 「遠端收集器管理員」發生例外

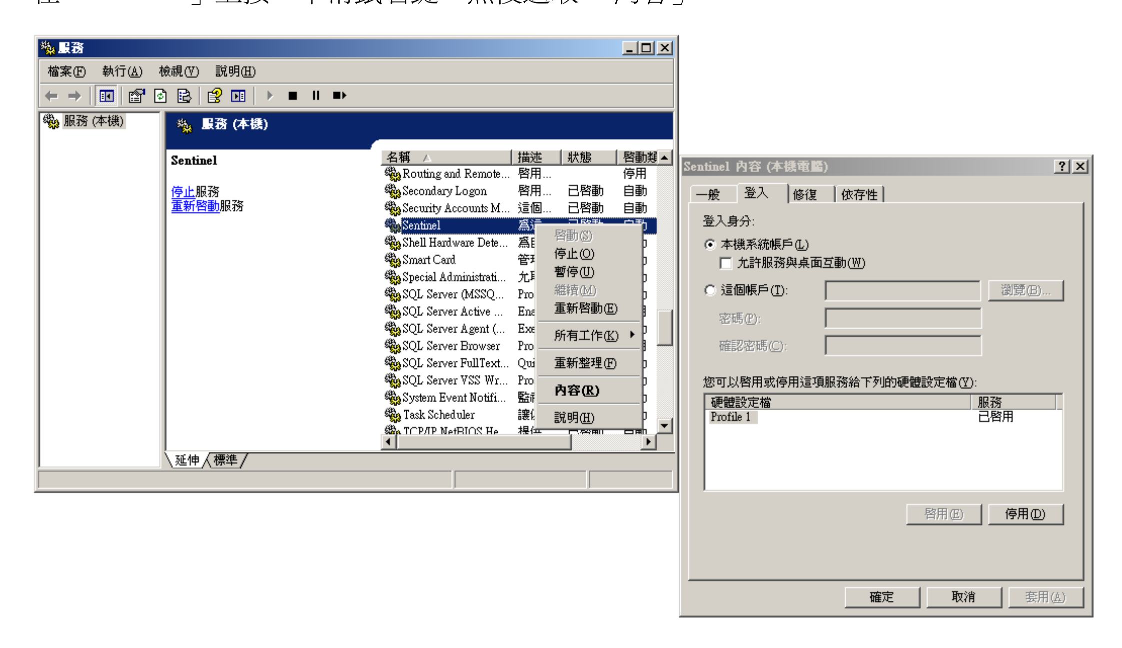
問題： 以屬於 「管理員」群組的使用者身分登入，然後在終端機提示字元中執行 setup.bat 指令以安裝收集器管理員。重新啓動系統或手動啓動 「收集器管理員」服務，然後以相同的使用者身分證明登入。例外將記錄在 collector_manager0.0.log 中，該檔案將影響以下收集器管理員功能：

- 映射未啓始化。
- 您無法使用 「檔案連接器」來選擇 「收集器管理員」 (Win2008) 機器之檔案系統上的任何事件來源檔案。

常見原因：您在 Windows 2008 SP1 標準版 (64 位元) 上安裝 「收集器管理員」。依預設，機器已將使用者存取控制 (UAC) 設定爲 *「已啓用」*。

動作：將 Sentinel Rapid Deployment 服務的 *「登入」*擁有者變更爲目前使用者。依預設，*「登入」*擁有者是設定爲 *「本機系統帳戶」*。若要變更預設選項：

1. 執行 services.msc 以開啓 *「服務」*視窗。
2. 在 「Sentinel」上按一下滑鼠右鍵，然後選取 *「內容」*。



3. 在 「Sentinel 內容」視窗中，選取 *「登入」*索引標籤。
4. 選取 *「這個帳戶」*，然後提供目前使用者 (您用來安裝 「收集器管理員」的使用者) 的身分證明。

B.4 未針對影像的收集器管理員建立 UUID

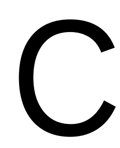
如果爲收集器管理員伺服器建立影像 (例如使用 ZenWorks Imaging 建立) 並將影像還原到其他機器，則 Sentinel Rapid Deployment 無法唯一識別收集器管理員的各個新例項。造成這一問題的原因是 UUID 出現重複。

您必須在新安裝的收集器管理員系統上執行以下步驟，才能產生 UUID ：

1. 刪除位於 <安裝目錄>/data 資料夾中的 host.id 或 sentinel.id 檔案。
2. 重新啟動收集器管理員。

   收集器管理員將自動產生 UUID。

維護 PostgreSQL 資料庫的最佳實務



您可以微調資料庫，以提高資料庫伺服器的效能。本章節中所述的限制是一些近似建議值，而並非絕對限制。不過，在高度動態的系統中，最好設定一些緩衝，以便為系統擴展預留空間。

C.1 修改記憶體組態參數

若要微調 PostgreSQL 資料庫伺服器，請在 < *安裝目錄* >/3rd party/postgresql/data/postgresql.conf 檔案中修改以下記憶體組態參數：

- **shared_buffers** ： 確定 PostgreSQL 用於快取資料的記憶體大小。為獲取較佳的效能，您可以將此參數值設定為可用 RAM 容量的四分之一。
- **effective_cache_size** ： 確定作業系統可在資料庫內進行磁碟快取的記憶體大小。您可以考量作業系統及其他應用程式所佔用的容量，預估出此參數的大小。可以將系統可用記憶體總大小的二分之一配置給此參數。
- **work_mem** ： 確定在切換至暫存磁碟檔案之前內部排序操作與雜湊表格所佔用的記憶體大小。該值以 KB 為單位加以指定。預設值為 1024 KB (1 MB)。

  如果是複雜查詢，可以同時執行多項排序或雜湊操作。各項操作都可以使用 work_mem 指定的記憶體大小，超過這一大小才會開始將資料放入暫存磁碟檔案中。如果在 Sentinel Rapid Deployment 系統上排程更多報告，請將此值設為介於 500MB 與 1GB 之間。
- **maintenance_work_mem** ： 確定要在資料庫維護操作 (如 VACUUM、CREATE INDEX 及 ALTER TABLE ADD FOREIGN KEY) 中使用的最大記憶體大小。該值以 KB 為單位加以指定。預設值為 16384 KB (16 MB)。

  將該設定設為較大的值可能會提高執行資料刪除及還原資料庫傾印操作的效能。不必變更此參數，因為預設值足以滿足 Sentinel Rapid Deployment 操作所需。

C.2 降低 Vacuum/Analyze 的 I/O 影響

您可以採用多種方式來提高 PostgreSQL 資料庫的效能。

- 下面兩個參數可以控制自動 vacuum 作業，依預設，這兩個參數在 Sentinel Rapid Deployment 伺服器安裝期間會被註釋，而您必須移除註釋並設定相應的值。
  - **vacuum_cost_delay** ： 決定當超出成本限制時程序休眠的時間長度。例如，您可以將此值設定為 100。
  - **vacuum_cost_limit** ： 決定導致 vacuum 程序休眠的累積成本。例如，您可以將此值設定為 10000。

    如果將這兩個參數的值設定為非零值，則可以降低 vacuum 與 analyze 指令對一般資料庫活動造成的 I/O 影響。執行報告時，它們對效能造成的影響可以忽略不計，因為 vacuum 所需的時間比以往長。

- 依預設，autovacuum 程序設定為 true，並且會定期執行以恢復磁碟空間及更新規劃器統計資料。隨著資料庫大小的增加，autovacuum 將無法維護保存所有資料庫物件。在此情況下，如果效能較慢，請以 cron 工作的形式執行 AnalyzePartitions.sh 程序檔。此 cron 工作應由擁有 Sentinel Rapid Deployment 程序的使用者進行設定。

  例如：

  ```
  30 11 * * * $ESEC_HOME/bin/AnalyzePartitions.sh
  ```

  其中：

  - 30 為分鐘時間。
  - 11 為小時時間。
  - ESEC_HOME 為資料庫的絕對路徑。

  在此範例中，程序檔於每日 11:30 執行。

- 避免將歸檔排程在報告作業期間執行。如果同時排程這兩個程序，報告將因 PostgreSQL 錯誤而進入等待狀態，並將在歸檔工作完成後才開始處理資料。此變更會影響資料庫的效能。